TRABAJO ESPECIAL DE GRADO

EVALUACIÓN DE IMPACTO DE IMPLANTACIÓN DEL DIRECCIONAMIENTO IPv6 EN LA RED DE SERVICIOS DE CANTV

Presentado ante la ilustre
Universidad Central de Venezuela
Por el Br. Expósito G., Gustavo A.

Para optar al título de
Ingeniero Electricista

Caracas, 2009

TRABAJO ESPECIAL DE GRADO

EVALUACIÓN DE IMPACTO DE IMPLANTACIÓN DEL DIRECCIONAMIENTO IPv6 EN LA RED DE SERVICIOS DE CANTV

PROFESOR GUÍA: Ing. William Jota
TUTOR INDUSTRIAL: Ing. Janette Oberto

Presentado ante la ilustre
Universidad Central de Venezuela
Por el Br. Expósito G., Gustavo A.
Para optar al título de
Ingeniero Electricista

Caracas, 2009

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELECTRICA
DEPARTAMENTO DE COMUNICACIONES

CONSTANCIA DE APROBACIÓN

Caracas, 25 de marzo de 2009

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Gustavo Expósito titulado:

"EVALUACIÓN DE IMPACTO DE IMPLANTACIÓN DEL DIRECCIONAMIENTO IPv6 EN LA RED DE SERVICIOS DE CANTV"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Luis Fernández
Jurado

Prof. Zeldivar Bruzual
Jurado

Prof. Willian Jota
Prof. Guía

Edificio Escuela de Ingeniería Eléctrica, piso 1, oficina 201, Ciudad Universitaria, Los Chaguaramos, Caracas 1051, D.F.
TELÉFONOS. (VOZ) +58 212 6053300 (FAX) +58 212 6053105
Mail: eie-com@elecrisc.ing.ucv.ve

DEDICATORIA

El siguiente trabajo se lo dedico a mis padres José y Amparo María, por su apoyo incondicional a lo largo de todos estos años.

RECONOCIMIENTOS Y AGRADECIMIENTOS

En primer lugar les agradezco a mis padres por su soporte debido al cual he podido culminar mis estudios.

A los miembros de CANTV que me brindaron su valiosa ayuda, entre ellos: Carmen Villavicencio, Yemi Salazar, Ender Mujica, Dayana Vásquez, Jesús Alberto Tovar, Jean Carlos Mena y muy especialmente a Janette Oberto y Carlos Camacho.

María Auxiliadora Rojas por su gran ayuda en el departamento de comunicaciones EIE UCV.

A William Jota por su todo su soporte y ayuda en la realización de este trabajo de grado.

Durante todos estos años en la universidad he tenido la gran fortuna de contar con el apoyo de amigos sin los cuales no hubiera podido completar mis estudios: José Barillas, Luis Maracara (QEPD), Rafael Rodríguez, Manuel Albornoz, Ángel Rodríguez, Gabriel Suarez, Jorge Pacheco Aguirre, Juan Rafael Ruiz.

Y finalmente, a los amigos con los que siempre conté: Juan Carlos Nuñez, Ignacio Mora, Antonio Beiro, Heidi Schlaya, Denisse Palacios, Virginia Silva, Paula Acevedo, Nathalie Ledezma, Natalia Falcone y su familia.

Expósito G., Gustavo A.

EVALUACIÓN DE IMPACTO DE IMPLANTACIÓN DEL DIRECCIONAMIENTO IPv6 EN LA RED DE SERVICIOS DE CANTV

Profesor guía: Ing. William Jota. Tutor Industrial: Ing. Janette Oberto. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: Compañía Anónima Nacional Teléfonos de Venezuela. Trabajo de Grado. 2009. 137h

Palabras Clave: Protocolo IPv6, coexistencia de protocolos, backbone, capa 3 del modelo OSI, conectividad entre redes.

Resumen. El presente trabajo de grado consiste en la evaluación del impacto en la red de servicios de CANTV al enfrentar el proceso de migración al nuevo protocolo de direccionamiento IPv6 manteniendo la coexistencia con el protocolo IPv4. Debido al agotamiento de las capacidades de direccionamiento del protocolo actual, a nivel global se converge en la solución de usar IPv6 que es prácticamente inagotable. Para la realización de este estudio primero se da a conocer los fundamentos de funcionamiento de las redes paquetizadas y los protocolos IPv4 e IPv6, luego se estudia la red de datos física y los servicios de la corporación, haciendo énfasis en la tecnología de enrutamiento que aplica en cada una de sus partes. De los servicios se estudia el funcionamiento de los mismos con IPv6 y que ventajas se pueden obtener de este protocolo que justifiquen la migración. Luego se identifican que partes de la red se ven afectadas y se estudia si es posible la operación de las mismas con el nuevo protocolo y que se requiere para esto. Toda migración trae consigo riesgos y áreas de atención que son analizadas en este estudio. Finalmente después de analizar las estrategias de migración mas comúnmente usadas, se recomiendan la conversión del back-bone a dual stack mediante la configuración en 6PE de los routers en el borde del mismo, para luego preparar los servidores DNS y DHCP, obteniendo así conexión a internet IPv6. Los servicios VoIP e IPtv pueden entonces comenzar a ser migrados en el momento que sea mas conveniente a la corporación.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ACRÓNIMOS

ABA	Acceso Banda Ancha
ADSL	Asymmetric Digital Subscriber Line
ARPA	Advansed Research Proyect Agency
AS	Autonomous System
ATA	Analog Telephone Adapter
ATM	Asincronic Transfer Mode
BGP	Border Gateway Protocol
BIND	Berkeley Internet Name Domain
BRAS	Broadband Remote access Aggregation
CDT	Clase de Tráfico
CE	Costumer Edge
CLI	Command Line Interface
CNR	Cisco Network Registrar
CPE	Costumer Premises Equipement
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EGP	External Gateway Protocol
GAN	Global Area Network
HTTP	Hiper Text Terminal Protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Internal Gateway Protocol
IHL	IP Header Length
IOS	Internetwork Operating System
IP	Internet Protocol
IPtv	Internet Protocol television
ISATAP	Intra Site Automatic Tunnel Addressing Protocol
IS-IS	Intermediate System to Intermediate System
ISO	International Organization for Standardization
ISP	Internet Service Provider
LACNIC	Latin American and Caribbian Internet Addresses Regitry

LAN	Local Area Network
LER	Label Edge Router
LS	Límite de Saltos
LSP	Label Switching Protocol
LSR	Label Switching Router
MAC	Media Access Control code
MAN	Metropolitan Area Network
MGW	Media Gateway
MLD	Multicast Listener Discovery
MPEG	Moving Picture Experts Group
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NAT-PT	Network Address Translation - Protocol Translation
NGN	Next Generation Networks
OCMP	Open Call Media Plataform
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PAN	Personal Area Network
PE	Provider Edge
PIM-SM	Protocol Independent Multicast - Sparse Mode
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point to Point Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAM	Random Access Memory
RIP	Routing Information Protocol
SBC	Session Border Controller
SC	Siguiente Cabecera
SDH	Synchronous Digital Hierarchy
SIP	Session Initiation Protocol
SOA	Start Of Authority
SONET	Synchronous Optical Network
SSH	Secure Shell
STP	Set Top Box
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDV	Tiempo de Vida
UDP	User Datagram Protocol

URL	Uniform Resourse Locator
VoD	Video on Demand
VoIP	Voice over Internet Protocol
VPLS	Virtual Private LAN Switching
VPN	Virtual Private Network
WAN	Wide Area Network
WWW	World Wide Web

INTRODUCCIÓN

Desde que se implementó IPv4 *(Internet Protocol version 4)* como protocolo de direccionamiento de redes e internet y debido al rápido crecimiento de esta última ya se puede vislumbrar el desbordamiento de las capacidades de dicho protocolo para el año 2011. Este tiene una capacidad total de 4.294.967.296 (2^{32}) direcciones de las cuales la IANA y sus divisiones regionales como LACNIC para Latinoamérica, han asignado aproximadamente la mitad del "pool" global de estas a los distintas ISP *(Internet Service Provider)*. Sin embargo, dado el crecimiento acelerado de redes conectadas a internet y debido a la adhesión de nuevos dispositivos y servicios como voz sobre IP *(Internet protocol)*, IPtv *(televisión via IP)*, juegos en línea, acceso de banda ancha a nivel de los hogares, escuelas y mayores exigencias de conectividad a nivel industrial, así como la revolución de los dispositivos móviles como celulares con conexión a internet, Wi-fi, Wimax, dispositivos de seguimiento de automóviles y electrodomésticos, se debe adoptar un nuevo protocolo de capa de red que permita una gran cantidad de hosts a nivel global. Este es IPv6, adoptado por el IETF *(Internet Engineering Task Force)* en 1994. No es sino hasta el año 2004 que la ICANN *(Internet Corporation for Assigned Numbers and Names)* parte de IANA *(Internet Assigned Numbers Authority)* anunció que los servidores raíces DNS *(Domain Name Server)* habían sido modificados para soportar ambos protocolos (registros AAAA para IPv6) y actualmente sólo unas pocas redes privadas y de nivel experimental lo han implementado, siendo el continente asiático quien lidera este proceso.

IPv6 consta de direcciones de host de 128 bits a diferencia de los 32 bits de IPv4. Esto implica 2^{128} direcciones posibles (aproximadamente 340 sextillones) o 670 mil billones de direcciones por milímetro cuadrado de la superficie terrestre. En pocas palabras la capacidad de hosts en la red global deberá dejar de ser un problema.

Entre otras características de IPv6 con respecto a IPv4 (aparte de la capacidad), se encuentra una cabecera de 40 bytes mas simplificada que ha eliminado

el “checksum” delegando la corrección de errores a las capas superiores, El campo de fragmentación también ha sido eliminado, por lo que los routers ya no cumplirán con esta función la cual queda delegada al dispositivo de origen. Este, dado el caso, creará una “cabecera de extensión” con la información requerida para recomponer la información en el destino. Estas cabeceras son otra de las innovaciones del protocolo: mediante la activación de un campo llamado “next header”, se pueden añadir nuevos campos opcionales al final de la cabecera IP y antes de la cabecera de la capa superior. Estas cumplen funciones como la ya nombrada fragmentación, seguridad, movilidad y ruteo. También se añade la “etiqueta de flujo” con funciones de calidad de servicio.

El proceso de cambio de protocolo se hará de manera gradual conforme se vaya agotando el pool actual de direcciones IPv4 el cual se ha mantenido debido a las restricciones impuestas por la IANA al reparto de las mismas, así como el amplio uso de técnicas como NAT *(Network Address Translation)* que enmascara redes que usan direcciones privadas internas y sólo usan una o algunas pocas direcciones públicas para conectarse a internet. Sin embargo esto rompe con la idea originaria de internet donde todos pueden conectarse con todos.

La corporación CANTV está al tanto del problema de agotamiento de las capacidades de IPv4, por lo que ha emprendido la labor de prepararse para la migración de protocolo, de manera de garantizar a su clientela conectividad total con las nuevas redes IPv6 que existen actualmente y las que con seguridad se crearán prontamente ofreciendo una nueva generación de servicios y aplicaciones. Este proceso se ejecutará en coexistencia con IPv4 y de la manera más transparente posible para el usuario final.

El presente trabajo tiene como objetivo general la evaluación de impacto de implantación IPv6 en la red de servicios de CANTV. Esto comprende el estudio de la red de datos y servicios con el objeto de evaluar las condiciones y métodos necesarios para la implementación de IPv6. En tal sentido los objetivos que inicialmente se plantean para alcanzar tal fin son los siguientes:

- Realizar un análisis comparativo entre los protocolos IPv4 e IPv6, características de ambos en función de los servicios ofrecidos por CANTV así como posibles beneficios y mejoras a estos.

- Evaluar las diferentes redes y servicios existentes y en vías de desarrollo e identificar y cuantificar los que se verán afectados por la migración, investigar las condiciones necesarias para que operen bajo el nuevo protocolo.

- Evaluar áreas de atención y riesgos.

- Generar recomendaciones para facilitar la implantación del nuevo direccionamiento en CANTV, a partir de las diferentes técnicas que permiten una coexistencia de ambos protocolos hasta lograr el establecimiento definitivo de IPv6.

CAPÍTULO I

MARCO TEÓRICO

1.1 Redes de Datos

El conjunto de dispositivos (llamados nodos) como computadores personales, impresoras, teléfonos digitales y routers, entre otros, interconectados mediante medios físicos de naturaleza eléctrica por los cuales intercambian información en formatos digitales se les denomina redes de datos.

Estas redes representan hoy en día una parte cotidiana y fundamental de la sociedad humana; están presentes en todas las actividades de esta, desde el comercio hasta el transito vehicular.

Existes dos clases de redes las cuales se diferencian entre sí por la manera como se transmite la información de un punto a otro; estas son redes de conmutación de circuitos y de conmutación de paquetes.

1.1.1 Conmutación de Circuitos

Se trata de la clase mas antigua de redes. Consiste en el establecimiento de caminos físicos entre los dispositivos que se deben comunicar, para esto diversos nodos intermedios actúan como switches que interconectan los medios que se requieren en el momento que se debe establecer una conexión y se liberan en el momento que la transmisión de datos finalizó. Un ejemplo de estas redes es el PSTN *(Public Switched Telephone System)* que enlaza equipos como Fax y módems del tipo dial-up. Actualmente aunque estas redes se encuentran muy difundidas en el mundo entero y su infraestructura se sigue usando para las comunicaciones de voz

analógicas, la tendencia está dada a sustituirlas por redes de conmutación de paquetes.

1.1.2 Conmutación de Paquetes

Este el tipo de red de mayor auge mundial, su ejemplo mas conocido es la Internet, las tendencias actuales van en el sentido de migrar sistemas como el de telefonía, radio y televisión a esta tecnología de red.

El funcionamiento de las mismas se basa en el enrutamiento de paquetes, los cuales son grupos de datos originados por una aplicación ubicada en un nodo que se comunica con otro en la red a la que pertenece; para esto dicha aplicación divide en un tamaño manejable por los nodos del sistema a la información total que se debe transmitir y le añade una dirección de origen y una de destino, las cuales son únicas dentro del alcance de la red. Los nodos intermedios pueden leer estas direcciones y tomar decisiones de por que vía enviar estos considerando el estado de la red para ese momento. No siempre todos los paquetes pertenecientes a una misma transmisión alcanzan su destino usando las mismas rutas físicas.

Una de las principales características de estas redes es la escalabilidad de las mismas Siempre y cuando se compartan protocolos comunes o compatibles y exista un direccionamiento único para cada nodo, se pueden ampliar o interconectar diferentes redes de manera casi automática.

Los componentes principales de estas redes se listan a continuación:

- *Host*: se trata de un nodo terminal de la red el cual recibe y transmite datos, como puede ser un computador personal o un *servidor,* el cual es un computador que trabaja de manera automática atendiendo pedidos de los usuarios de la red y llevando funciones de gestión de la misma.
- *Router*: nodos que básicamente son computadoras con la única finalidad de dirigir el tráfico de paquetes en base a unos protocolos preestablecidos en su configuración, Para esto recopilan información acerca del estado de

la red de manera continua y calculan las vías optimas de retransmitir los paquetes que reciben.

- *Medio o Link*: es la conexión física entre los nodos, pueden ser de cualquier tipo de interconexión eléctrica como radio, fibra óptica o cobre. Estos son compartidos por dos o mas elementos por lo que están sujetos a protocolos de acceso cuyo alcance es local para dicho medio. Se considera que los diferentes terminales de un router representan links distintos aunque estos sean del mismo tipo físico, en otras palabras redes o sub-redes distintas.
- *Puente*: en ocasiones se requiere que la información cambie de medio y por lo tanto de protocolo de acceso, estos dispositivos se ocupan de mantener la compatibilidad entre ambos medios.
- *Hub*: dispositivos repetidores, estos copian cada paquete recibido por alguno de sus terminales y lo reenvía al resto de ellos. El hub se puede considerar parte del link ya que es transparente a los dispositivos conectados a este.
- *Switch*: semejante al hub pero dotado con una mayor capacidad de procesamiento ya que puede elegir por cual terminal enviar un paquete debido a que "entiende" el protocolo usado por el link al que pertenece y conoce que dispositivos están en cada uno de sus terminales; esto para evitar un exceso de tráfico en el mismo.

Según su alcance las redes se clasifican de la siguiente manera:

- *PAN*: *Personal Area Network.* Red personal, esta compuesta por dispositivos portátiles.
- *LAN*: *Local Area Network.* Redes de alcance local.
- *MAN*: *Metropolitan Area Network.* Comprende las redes de distribución a nivel urbano de los proveedores de servicios de red o ISP (*Internet Service Provider*).

- *WAN*: *Wide Area Network.* Son las redes que interconectan a todas las anteriores, pueden tener alcance urbano o nacional, su principal característica es que carecen de enlaces multipunto.
- *GAN*: *Global Area Network.* Tienen las mismas características de una WAN pero con alcance internacional.

Los ISP *(Internet Service Provider)* poseen las redes mas grandes que pueden existir en un país. Estas dividen su red en varios sectores que se describen a continuación:

- *Core*: es el corazón de la red, también llamado backbone *(columna vertebral)*. Es un conjunto de routers interconectados que representan el principal bloque de transferencia de datos entre las redes de distribución, internet y redes de servicios y gestión. Se diseña de manera que siempre existan rutas redundantes entre las redes ya nombradas.
- *Borde de Internet*: frontera con las redes externas al ISP. Los routers que lo conforman se encuentran directamente conectados con otras corporaciones o ISP extranjeros o nacionales. Estos routers están sujetos a protocolos de funcionamiento especiales.
- *Distribuidor de Internet*: interconexión entre el core y el borde de internet; sobre éste recaen funciones de gestión.
- *Distribución:* conexión del core con las distintas redes que llevan el acceso a los usuarios finales.
- *Redes de gestión y servicios:* están conformadas por servidores y routers que se conectan directo al core. Estas proporcionan control y monitoreo de la red así como servicios como IPtv (*televisión vía Internet Protocol)* o VoIP *(Voz vía Internet Protocol)*.

1.2 El Modelo OSI

El modelo de interconexión de sistemas abiertos o *Open Systems Interconnection* es un estándar de la ISO *(International Standards Office),*que cubre todos los aspectos de las redes de comunicación. Su objetivo es proporcionar como su nombre lo dice un modelo de donde los distintos fabricantes puedan interconectar sus dispositivos sin importar el hardware o software subyacente a sus tecnologías, compartiendo protocolos comunes para cada parte de la comunicación establecida por este, aunque de por si no es un protocolo.

Tiene sus orígenes a finales de los años setenta cuando existía un gran auge en la implementación de redes para las industrias, universidades, gobiernos y militares, En aquel entonces habían tecnologías de red de gran alcance aunque lentas para los estándares de hoy en día; el gran problema recaía en que todas eran de carácter propietario y en consecuencia incompatibles entre sí. Entonces fue cuando intervino la ISO permitiendo que nacieran las redes que conocemos actualmente.

Es un modelo por niveles o capas que representan las diferentes etapas para conectar cualquier tipo de dispositivos. Estos cumplen tareas específicas y están relacionados unos con otros. En el proceso de transmisión de datos, estos pueden pasar por nodos intermedios como routers los cuales solo ejecutarán las primeras dos tres o cuatro capas.

Cada capa tiene asociado algunos protocolos y un formato para los datos que maneja, como se puede ver en la *tabla 1.1*:

Capa	Nombre	Tipo de Información	Ejemplos de Protocolos
L7	Aplicación	datos	DNS, FTP, HTTP, POP
L6	Presentación	datos	ASCII, MPEG
L5	Sesión	datos	NetBIOS, SAP
L4	Transporte	segmentos	TCP, UDP
L3	Red	paquetes	IP, ICMP, OSPF, IS-IS, appleTALK
L2	Enlace de Datos	trama	Ethernet, PPP, ATM, Frame Relay
L1	Física	bits	xDSL, SONET, T1, E1

Tabla 1.1 Modelo OSI [1]

1.2.1 Capa 7. Aplicación

Es la mas cercana al usuario final. Es el software de aplicación con el que el usuario interactúa y este a su vez implementa el proceso de comunicación al activar las capas inferiores; este usuario puede ser humano u otro software como es el caso de los servidores.

Sus funciones incluyen: identificar sus pares o aplicaciones asociadas en equipos remotos, determinar la disponibilidad de recursos y sincronizar la comunicación.

DHCP y DNS son ejemplos de protocolos de esta capa que debido a su importancia en esta investigación serán tomados en consideración mas detalladamente en este capitulo.

1.2.2 Capa 6. Presentación

Se trata de la manera o formato en que la información se dispone para ser transmitida, la sintaxis o semántica de esta para que sea entendida por ambas aplicaciones en comunicación.

Sus labores incluyen traducir los códigos recibidos transmitidos en el caso de que sean distintos pero compatibles. Cifrar información que se considere de carácter

privado. Es en esta capa donde las contraseñas introducidas en páginas web son encriptadas para evitar ser leídas por terceros. Comprimir la información para facilitar el transito de la misma en la red evitando la congestión de la misma, un ejemplo de esto es el video en comprimido en formato MPEG *(Moving Picture Expert Group)* que se usa en los servicios de IPtv.

1.2.3 Capa 5. Sesión

Establece mantiene y sincroniza la interacción entre sistemas de comunicación. Es un controlador del dialogo de red al permitir que dos procesos remotos tengan comunicación. Otra de sus funciones consiste en la sincronización del flujo de datos a la aplicación añadiendo y leyendo *chek-points* cada cierta cantidad de datos transmitidos con la finalidad de verificar la integridad de la información recibida.

1.2.4 Capa 4. Transporte

Se encarga de segmentar la información en segmentos manejables por la red y darles un número de secuencia a cada uno de estos con el cual se puede reconstruir la información recibida al ordenar, sustituir los segmentos perdidos y descartar los duplicados.

En un host puede haber distintas aplicaciones comunicándose a la vez; esto implica que habrá varios flujos de segmentos para cada una de estas. Para poder diferenciarlos la capa de transporte añade un identificador único por aplicación a estos flujos permitiendo el correcto re-ensamblaje de estos y la entrega las capas superiores.

El control de conexión es otra de las funciones de esta capa. Esta puede ser orientada a la conexión o no. En el primer caso los protocolos de *L4* deben establecer un dialogo con el host remoto para verificar si está preparado para la comunicación y solicitar o enviar acuses de recibo de los segmentos enviados. Una vez terminado el

proceso se realiza la desconexión. En el caso no orientado a la conexión simplemente se envían o reciben segmentos sin esperar o enviar confirmaciones ni verificar el estatus del host remoto.

Al igual que en la capa superior ésta cumple funciones de corrección de errores al verificar la integridad del segmento recibido así como la posible duplicación o perdida de los mismos. Para corregir estos se solicita la retransmisión de los segmentos afectados.

1.2.5 Capa 3. Red

Se ocupa de entregar la información de origen a destino en la red, Para esto toma los segmentos de la capa de transporte y les añade direcciones de origen y de destino; hecho ésto dichos segmentos pasan a llamarse paquetes. Los dispositivos intermediarios de la red o routers pueden tomar estas direcciones y encaminar los paquetes hacia su destino final.

La importancia de este protocolo recae en que permite crear *redes de redes* al permitir la interconexión. Una red que no requiera adherirse a otras puede suprimir esta capa del modelo ya que, como se verá en el siguiente punto, la información se puede direccionar de manera local con *direcciones físicas*, pero se pierden las características de escalabilidad que proporcionan las *direcciones lógicas* de la capa de red. Se denominan lógicas ya que no están relacionadas con ningún tipo de hardware y no necesariamente pertenecen a un host específico de manera permanente.

En estas direcciones, su característica mas importante es que no solo identifican al host si no a la red a la que pertenece de manera única en el alcance de la red de redes en que se encuentra. Es esta característica la que permite el enrutamiento de paquetes a redes remotas.

1.2.6 Capa 2. Enlace de Datos

El alcance de esta capa no supera al de la red o sub-red local; en otras palabras se ocupa de controlar el acceso de la información al medio al cual están conectados dos o más nodos de red y procura la entrega segura de la información de nodo a nodo en el link.

Para transmitir en el medio, *L2* divide el flujo de información proveniente de la capa de red en *tramas* las cuales no tienen que contener necesariamente paquetes completos. Estas tramas poseen una dirección física de origen y una dirección física de destino, las cuales son únicas para el medio al que están conectados sus respectivos dispositivos. Estos permanecen todo el tiempo leyendo o "escuchando" la información que se transmite por el medio, cuando escuchan que la dirección de destino es la propia, entonces procesan la trama a la capa superior retirando la información introducida por la capa de enlace de datos, caso contrario descartan la trama. En el caso de que la información tenga como destino un enlace fuera de la red local, la dirección de destino será la del dispositivo capaz de conectarse con otras redes, como puede ser un router.

Suele suceder que los dispositivos conectados a un medio no llevan la misma velocidad de lectura o escritura. Para evitar un desbordamiento de información esta capa impone algún método de control de flujo.

Para garantizar la entrega segura se incluyen mecanismos de detección de tramas corruptas o duplicadas mediante la agregación una "*cola"* o datos que se añaden al final de la trama.

Un problema obvio de conectar varios dispositivos a un mismo medio recae en que solo uno puede transmitir a la vez. La responsabilidad de establecer mecanismos que coordinen el acceso al medio pertenece a esta capa

.

1.2.7 Capa 1. Física

Trata directamente con las características del medio en que se transmite la información, tanto en sus características eléctricas como sus características mecánicas. Es la manera como se representan los ceros y unos (o grupos de estos que formen códigos) de las señales digitales, como puede ser en amplitud, frecuencia o fase. También son tareas de esta capa la sincronización, así como la tasa de datos o el tiempo que dura cada bit en el medio,.

A partir de la creación del modelo OSI, los protocolos nacientes usarán como referencia la estructura por capas para facilitar la distribución de tareas. A pesar de esto el modelo TCP/IP no cumple a cabalidad el lineamiento dado en el modelo OSI ya que fue implementado tiempo antes que este.

1.3 Internet y el Modelo TCP/IP

Internet o *red de redes* como su nombre lo dice se trata de un grupo diverso de redes interconectadas, en donde cada red y host perteneciente a estas se encuentra identificado de manera única. La internet mas conocida es la global o *World Wide Web* que se puede resumir como una gran interconexión de los diversos ISP y corporaciones mundiales, mayoritariamente mediante fibras ópticas que atraviesan el fondo de los océanos y no posee un control centralizado del cual dependan todas las interconexiones.

En el año 1969 el departamento de defensa de los Estados Unidos de Norte América y su Agencia de Proyectos de Investigación Avanzada ARPA *(Advansed Research Proyects Agency)*, crearon la primera red de conmutación de paquetes mediante enlaces punto a punto alquiladas y sin depender de un único punto de control y gestión, la cual se denomino *Red de la Agencia de Proyectos de Investigación Avanzada*. De esta red surgieron una serie de convenciones que hoy en día se conocen como el conjunto de protocolos TCP/IP. En los años ochentas las comunidades universitarias en el mundo adoptaron esta tecnología para interconectar

las redes de los diversos campus usando mayoritariamente como enlaces la red PSTN. De allí surgieron el resto de los protocolos con que hoy la internet global puede operar.

Se puede observar en la *tabla 1.2* las partes del modelo TCP/IP, cabe destacar que para el punto de vista de estos protocolos la internet es una "gran red" y no una serie de redes interconectadas.

Capa	Nombre	Tipo de Información	Ejemplos de Protocolo
4	Aplicación	Mensaje	HTTP, DNS, DHCP
3	Transporte	Segmento o Datagrama de Usuario	TCP,UDP
2	Internet	Paquete	IP
1	Enlace	Trama	Ethernet, PPP, ATM, Frame Relay

Tabla 1.2 Modelo TCP/IP [2]

Dado que el modelo TCP/IP existe desde antes que el modelo OSI, estos no coinciden exactamente, sin embargo al TCP/IP se le puede considerar como una particularidad del OSI.

1.3.1 Capa Aplicación

De igual manera que en el modelo OSI representa el software que interactúa con el usuario o con otro software. Esta capa incluye a los programas que responden de manera automática a las peticiones realizadas a un servidor, solo que ahora la unidad de datos tomará el nombre de *mensaje*. DNS y DHCP pertenecen a esta capa.

1.3.1.1 Sistema de Nombres de Dominio

Mejor conocido DNS, es un protocolo de estructura jerárquica que se encarga de resolver las direcciones IP para un URL *(Uniform Resourse Locator),* el cual es el nombre de algún servicio como una página web o una dirección de correo electrónico. Esto permite que los usuarios no necesiten recordar complicadas direcciones numéricas; en lugar de eso tendrán en cuenta nombres mas fáciles de recordar. Estos URL están registrados en bases de datos alojadas en los servidores DNS, los cuales actúan como las guías telefónicas de internet. Estos están dispuestos de manera jerárquica por el dominio que representen o para el cual son autoritativos; por ejemplo la dirección *http://neutron.ing.ucv.ve/* posee cuatro dominios, siendo *.ve* el de mayor rango y perteneciente a un *servidor raíz*, para el cual ese dominio es autoritativo, *.ucv* pertenece a un servidor DNS del campus universitario, *.ing* pertenece a la facultad de ingeniería, cada registro en las bases de datos de estos hacen referencia a los registros almacenados en los servidores de rango inmediato inferior.

Cuando un usuario realiza una consulta DNS, el software de host realiza un llamado al servidor que se encuentra establecido por defecto en su configuración de red el cual puede ser el que proporciona el ISP. Este verifica primero si el URL pertenece a un dominio local, si no es así realiza una consulta a un servidor raíz de los trece que existen en el mundo [3], (algunos son en realidad grupos de servidores) Entonces, si este no posee el URL en cuestión envía al DNS local la dirección de otro DNS perteneciente al dominio de mayor jerarquía en el URL. El proceso se repite hasta dar con el servidor *autoritativo*. Una vez resuelta la dirección IP de un URL esta queda grabada como una dirección *no autoritativa* en el servidor local por un tiempo específico previniendo que exista mas tráfico hacia esa locación de internet con fines de optimizar el proceso.

Entre los registros más comunes se encuentran NS, MX, HINFO, A y AAAA de los cuales los dos últimos guardan las direcciones IPv4 e IPv6 respectivamente para cada URL.

1.3.1.2 Protocolo de Configuración Dinámica de Host

Para que un host se conecte a una red, este requiere de una dirección IP. Esta se puede obtener mediante una asignación previa de manera permanente o *estática* o mediante DHCP *(Dinamic Host Configuration Protocol)*. Mediante este protocolo el host adquiere una dirección IP por un período de tiempo específico al termino del cual cabe la posibilidad de renovar la misma. Son los hosts como computadores personales y estaciones de trabajos los que requieren de este servicio. Los dispositivos como routers o servidores que se mantienen conectados a toda hora poseen direcciones IP estáticas lo cual facilita las labores de gestión de los mismos.

Para poder asignar direcciones IP con este protocolo se requiere de un servidor DHCP; este es aportado por el ISP o por el proveedor de servicios de red. Un host que aun no posee dirección IP no se puede conectar fuera de la red a la que pertenece pero si a esta con el uso de la dirección L2 o *dirección MAC (Media Access Control)*. Se envía una solicitud llamada *descubrimiento DHCP;* si existe un servidor en la misma red este responderá con una *oferta* en el cual se identifica y le ofrece una dirección IP, una *mascara de sub-red* y una dirección de servidor DNS, el host verifica que esta IP alquilada sea única y acorde a la red que pertenece y entonces envía un mensaje de *reconocimiento* con la cual el servidor reserva la dirección previamente ofrecida para el host dado.

En el caso de que no exista un servidor DHCP en la red, los routers están configurados como agentes relevadores reenviando los mensajes oferta DHCP a un servidor en otra red cuya dirección le es conocida.

1.3.2 La Capa de Transporte

Realiza las mismas funciones de L4 en el modelo OSI. Los protocolos de esta capa coordinan comunicaciones llamadas *conversaciones* entre las aplicaciones de hosts distintos en una internet las cuales están identificadas por un *número de puerto* de 16 bits, los que nos da 65.535 [4] puertos distintos; de estos los que van del 0 al

1023 son los llamados *bien conocidos* e identifican las aplicaciones en los servidores (por ejemplo el 80 identifica una aplicación HTTP), Del 1024 al 49151 son los puertos *registrados* para identificar las aplicaciones a nivel de usuario y suelen ser asignados de manera dinámica, por último los restantes son los puertos *privados* de libre uso por aplicaciones no reconocidas por la IANA *(Internet Assigned Numbers Authority),* quien es la autoridad que asigna los números de puertos explicados anteriormente.

1.3.2.1 El Protocolo TCP

Transmission Control Protocol o protocolo de control de transmisión tiene como característica estar orientado a la conexión. Cuando el usuario solicita una conversación con un host remoto, éste establece una sesión en donde coordina con sur par remoto la forma en que se van a transmitir los datos y las numeraciones a usar para identificar la secuencia de datagramas (que permite la reconstrucción del mensaje en el orden correcto), y los *acuses de recibo* necesarios para que el host que envía los datos sepa que puede seguir enviando información o caso contrario reenviar la que llegó corrupta o simplemente no llegó. También debe controlar el flujo de información coordinando entre ambos hosts el *tamaño de ventana* el cual es la cantidad de datagramas que se enviaran después de cada acuse de recibo y dependerá de las condiciones de la conexión. En la *tabla 1.3* se puede observar la cabecera TCP

<< ---------- 32 bits ---------- >>

Puerto de Origen		Puerto de Destino	
Número de Secuencia			
Número de Acuse de Recibo			
LCT | Reservado | Flags		Ventana	
Suma de Verificación		Puntero de Urgencia	
Opciones			Relleno

Tabla 1.3 Cabecera TCP [4]

De esta tabla, aparte de los campos explicados anteriormente, LCT *(Longitud del Cabezal TCP)* indica que tan largo es este cabezal y por lo tanto el inicio del segmento de datos, *reservado* se guarda para futuras aplicaciones, *flags* son indicadores varios usados para el proceso de conexión y desconexión, *suma de verificación* se requiere para verificar la integridad tanto del cabezal como los datos. Si la suma de verificación realizada por el receptor no coincide con la que esta en este campo el datagrama es descartado. El *puntero de urgencia* indica un flujo de información de carácter urgente, *opciones* información opcional (optativo).

1.3.2.2 El Protocolo UDP

Las funciones de transmisión segura con que cuenta el protocolo TCP traen como desventaja un mayor congestionamiento de la red y un retardo en el flujo de datos a consecuencia de la espera de acuses de recibo. Para aplicaciones de alto flujo de datos como un stream de video en donde la pérdida de cierto número de datagramas no significa la pérdida significativa de la calidad del mismo, se puede requerir de UDP *(User Datagarm Protocol),* Este es no orientado a la conexión en donde sus funciones se limitan a identificar las conversaciones a las que pertenecen los datagramas y verificar errores en los mismos, pero dado que los hubiese no solicita retransmisión. Se puede observar la cabecera UDP en la *tabla 1.4.*

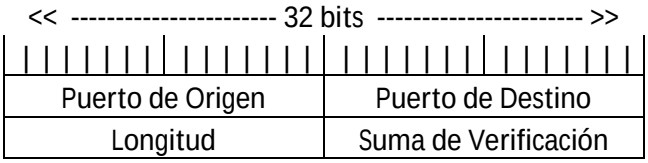


Tabla 1.4 Cabecera UDP [4]

1.3.3 La Capa de Internet

Esta es esencialmente igual a la L3 del modelo OSI, sólo que el protocolo a usar es el *protocolo de internet* o IP *(Internet Protocol)* el cual proporciona una forma de identificar a todos los dispositivos y a todas las redes pertenecientes a una internet, de manera única, con lo que el encaminamiento de paquetes a través de ella es posible.

Otra función importante de esta capa es el establecimiento de la mejor ruta para el tráfico de paquetes. Los routers requieren de mecanismos que les permitan elegir por donde enviar los paquetes que reciben, para esto construyen tablas de encaminamiento a partir de la información que reciben y comparten con routers vecinos. Los protocolos que pertenecen a la red interna de un ISP se denominan IGP *(Internal Gateway Protocol)*, los que funcionan en la interconexiones de estos se llaman EGP *(External Gateway Protocol)*, BGP *(Border Gateway Protocol)* es el único de estos últimos usados en internet. Los IGP se dividen en dos, los que toman las decisiones a partir de los *saltos* o cantidad de routers que debe atravesar un paquete para llegar a destino y los que lo hacen a partir de hallar las rutas con mejor ancho de banda. A los primeros se les denomina *protocolos de vector de distancia* y un ejemplo de estos es RIP *(Routing Information Protocol)* a los segundos se les denomina *protocolos de estado del vínculo* y son actualmente los mas usados por lo que se les dará una vista más cercana en los próximos puntos. Cabe destacar que estos pueden operar de manera conjunta en cada router, éste simplemente usará la

información que le proporcione el protocolo más confiable según se hayan configurado.

Se encuentra también en esta capa el protocolo ICMP *(Internet Control Message Protocol)* el cual se usa para enviar mensajes de error y obtener información de la red.

Se debe recordar que este protocolo no garantiza la entrega de paquetes, esa función queda delegada a la capa superior.

1.3.3.1 Protocolo de Internet Versión 4

Mas conocido como IPv4 *(Internet Protocol version 4)* surge a partir de protocolos de origen militar que requerían redes que no pierdan su conectividad a pesar de que partes de la red sean desactivadas. En 1981 la IETF *(Internet Engineering Task Force)* publica el RFC 791, naciendo así este protocolo que fue prontamente adoptado por las redes universitarias y por industrias de la informática como IBM.

Usa un direccionamiento de 32 bits, Estos dan una capacidad de direccionamiento máxima de 4.294.967.296 (2^{32}) hosts, Parece un número grande pero la realidad es que se ha quedado pequeño ante el rápido crecimiento de la red global. La notación mas común es la de dividir en 4 bytes y mostrar estos en notación decimal separada por puntos, por ejemplo 150.185.86.9 .

Los 32 bits están divididos en bits de host y bits de red. Los hosts pertenecientes a una misma red deberán tener los mismos bits de red pero siempre distintos bits de host. Para que un dispositivo pueda diferenciar la parte de red de la de host estos deben de conocer al momento de ser configurados la *mascara de sub-red* la cual son 32 bits de los cuales valen “1” todos aquellos que corresponden a la red y “0” los que corresponden a las direcciones de host. Estos se escriben con la misma notación de las direcciones, una simple operación lógica *and* entre ambos dará como resultado *la dirección de red*, la cual tiene como característica que todos los bits de host valen “0” mas no así los de red . Cuando todos los bits de host valen “1”

se tiene la dirección de *broadcasting*. Todos los paquetes enviados a esa red con esa dirección serán escuchados por todos los dispositivos que están conectados a la misma. Otra manera de indicar la mascara de sub-red es con una barra "/" a la derecha de la dirección IP indicando a continuación el número de bits de red.

Las direcciones IPv4 se dividen en clases según el tamaño de la red a la que pertenecen, según asignación de la IANA, estas clases son las indicadas en la *tabla 1.5*:

Clase	Rango de direcciones	prefijo de subred
A	0.1.0.0 >> 126.0.0.0	/8
B	128.0.0.0 >> 191.255.0.0	/16
C	192.0.1.0 >> 223.255.255.0	/24
multicast	224.0.0.0 >> 239.255.255.255	...
experimentales	240.0.0.0 >> 255.255.255.254	...

Tabla 1.5 Clases IPv4 [4]

Las direcciones de *multicast* son para enviar paquetes en broadcasting a diferentes redes al mismo tiempo, las direcciones *experimentales* son usadas por universidades y la industria de telecomunicaciones e informática con fines de desarrollo. Además existen grupos de direcciones privadas las cuales pueden ser libremente usadas por redes aisladas *(tabla 1.6)*, pero no en ningún internet, los routers que reciban un paquete con una de estas direcciones como dirección de origen no lo reenviaran. A continuación un ejemplo de las características del direccionamiento IPv4, *tabla 1.7*

Rango de direcciones	Prefijo de subred
10.0.0.0 >> 10.255.255.255	/8
172.16.0.0 >> 172.31.255.255	/12
192.168.0.0 >> 192.168.255.255	/16

Tabla 1.6 Direcciones Privadas [4]

dirección	clase	máscara de subred	Prefijo S-R
150.185.86.9/19	B	255.255.224.0	19
direccion-máscara de subred-subred (bits de red/bits de sub-red/bits de host)			
"10010110101110010101011000001001"			
"11111111111111111110000000000000"			
"10010110101110010100000000000000"			
subred	Cantidad de sub-redes	Cantidad de hosts	
150.185.64.0	8	8190	

Tabla 1.7 Ejemplo IPv4. Fuente: Autor.

El protocolo IPv4 agrega una cabecera al datagrama proveniente de TCP con toda la información requerida para el viaje de este a través de internet, misma información que retira al procesar paquetes recibidos. Esta cabecera tiene la siguiente forma *tabla 1.8*:

<< ---------- 32 bits ---------- >>

Ver. | IHL	Servicio	Longitud total
Identificación		Fragmentación
TDV	Protocolo	Suma de Cabecera
Dirección de Origen		
Dirección de Destino		
Opciones . . .		

Tabla 1.8 Cabecera IPv4 [4]

De esta tabla el campo *Ver.* (versión) es un indicador de que es un paquete IPv4, *IHL* es la longitud de la cabecera, el valor en *servicio* es un indicador de *QoS (Quality of Service)* el cual es usado por los routers para dar prioridad a unos paquetes en lugar de otros (por ejemplo un stream de video tiene prioridad frente a un mensaje de correo), en *longitud total* se observa el tamaño del paquete completo, con

identificación se reconocen los paquetes provenientes de un proceso de fragmentación y *fragmentación* indica el lugar de este paquete en dicho proceso, el campo *TDV* o tiempo de vida, disminuye en uno cada vez que un router lo reenvía, cuando vale cero es descartado, en *protocolo* se indica cual es la cabecera de la capa superior, *suma de cabecera* al igual que en TCP se usa para determinar la integridad del paquete y con *opciones* se añaden campos adicionales para diversos usos en caso de que apliquen.

1.3.3.2 Protocolo de Internet Versión 6

A principios de los años noventa cuando la red global comenzaba a crecer a gran velocidad se pudo vislumbrar lo que hoy es ya una realidad, el agotamiento de la capacidad de direccionamiento de IPv4. Bajo esta situación la IETF propulsó el desarrollo de un nuevo protocolo que resuelva este problema y añada algunas mejoras. En 1993 la organización comenzó con una investigación llamada IPng *(Internet Protocol next generation)*, al año siguiente esta arrojó la recomendación de implementar IPv6 y es en el año de 1998 en que éste y el conjunto de protocolos relacionados se convierten en estándar cuando la IETF terminó de publicar todos los *borradores* definitivos, siendo el RFC-2460 el que especifíca las características de este protocolo.

Ahora se disponen de 128 bits de direccionamiento, lo que nos da una capacidad total de 2^{128}, aproximadamente 340 sextillones lo que equivale a 670 mil billones de direcciones de por cada milímetro cuadrado del planeta. La capacidad de hosts deberá dejar de ser un problema.

La nomenclatura usada para estos 128 bits queda dada dividiendo estos en 8 grupos de 16 bits, escritos en formato hexadecimal y separados por “:” entonces tendrán la forma:

200E:AFF5:0000:06B0:0000:0000:0045:DC10

Estas a su vez pueden ser reescritas siguiendo las siguientes reglas: los ceros a la izquierda de cada grupo se pueden obviar, los grupos consecutivos de ceros se pueden sustituir por "::" pero sólo una vez. Aplicando esto se tiene:

200E:AFF5:0:6B0::45:DC10.

Para que un servidor DNS reconozca esta dirección esta debe estar encerrada entre corchetes, así se diferencia de una dirección IPv4 o de un URL, de esta manera:

http://[200E:AFF5:0:6B0::45:DC10]/index.html

En IPv6 las direcciones de *broadcast* ya no se usan mas, en su lugar se usan las direcciones de *multicast*, se mantienen las de *unicast* y se introducen un nuevo tipo, las *anycast*.

A diferencia de IPv4 se espera que cada interfaz en un nodo tenga mas de una dirección IPv6 de cualquier tipo. Las interfaces en enlaces punto a punto pertenecientes a los routers no poseen direcciones IPv6 ya que estos no son puntos de origen o destino para datagramas. Además se mantiene el uso del carácter " / " para indicar la parte de red y sub-red.

Excepto para multicast y anycast, todos los tipos de direcciones pueden usar *EUI-64 (Extended Unique Identifier 64)* para la parte de las interfaces o parte de host, llamada *interface-ID*. Esto es la dirección física MAC, propia del hardware de la interfaz de 48 bit a la cual se le añade el bloque hxFFFE después de los 24 bits de menor apreciación o bits del fabricante y antes de los 24 bits restantes o bits asignados por la IEEE *(Institute of Electrical and Electronics Engineers)*. Existen otras opciones para identificar la parte de host como lo son el uso de algún número que se genere aleatoriamente o una tabla de numeración estática.

Las direcciones unicast son para una única interfaz, existen varios tipos que varían según su alcance. *Global unicast* son el equivalente a las direcciones unicast en IPv4, estas tienen identificada la red a la que pertenecen por un grupo de prefijos diferenciados que se muestran a continuación en la *figura 1.1*:

Figura 1.1 Dirección Global Unicast [RCF 3587]

El prefijo 001 es el que permite reconocer a esta dirección como global unicast, El Prefijo de Ruteo Global *(Global Routing Prefix)* se divide en dos partes, el *Prefijo ISP* el cual es de longitud variable y es asignado por la IANA (actualmente se asignan /32) y el *Prefijo de Sitio* el cual pueden usar los ISP para organizar sus sub-redes, *Site ID* tiene como finalidad que algún cliente de ISP como una organización o agencia gubernamental cree y administre su propia jerarquía de red. Los primeros 48 bits son llamados *topología pública.*

Los routers guardan en su tabla de enrutamiento sólo la parte de las direcciones acorde al nivel al que pertenecen aumentando así la eficiencia de procesamiento y memoria. Por ejemplo los routers de borde de internet en un ISP sólo procesan los primeros 16 bits.

Se introducen como novedad con respecto a IPv4 dos tipos de direcciones de alcance limitado, *link-local* y *site-local*, para el enlace y para la organización. Las primeras son usadas para comunicaciones entre nodos vecinos conectados al mismo enlace en el proceso de *descubrimiento de vecindario* el cual es una característica de este protocolo en donde en ausencia de router los hosts pueden comunicarse entre ellos automáticamente, sin necesidad de configurarles ningún tipo de direcciones. Se reconocen por usar siempre el prefijo FE80::/16, los bits del resto de la parte pública y de sitio valen “0”.

Las direcciones site-local son usadas para comunicar nodos pertenecientes a una misma organización, los routers de borde no reenviarán paquetes con estas direcciones fuera de la misma, son el equivalente a direcciones privadas. Estas tienen como prefijo FEC0::/10, el resto de los bits de la parte pública se denominan *subnet ID* y se usan para crear sub-redes, es llamado también *identificador de alcance*.

Las direcciones *multicast* identifican a un grupo de interfaces en un alcance dado. Nodos localizados arbitrariamente pueden escuchar tráfico multicast en el alcance de este y a su vez puede escuchar diversos tráficos de este tipo por cualquiera de sus diversas direcciones multicast al mismo tiempo; estos también pueden añadirse o retirarse de un *grupo multicast* en cualquier momento. La estructura de estas direcciones se puede observar en la *figura 1.2*.

Figura 1.2 Dirección Multicast

"P" es el prefijo que identifica una dirección multicast, este es "1111 1111" , F o *flags* indican diferentes opciones como el status de transitoriedad de la misma, S o *scope* indica hasta donde puede llegar una transmisión, puede ser desde sólo el vinculo hasta global. El identificador de grupo es único en el alcance dado.

Las direcciones *anycast* son parte de las novedades de IPv6. Estas al igual que las multicast identifican a un grupo de interfaces, pero se diferencia en que estos no necesariamente pertenecen a una determinada región y el paquete solo llegará a una de estas, pueden existir dos direcciones anycast iguales pero los paquetes se encaminaran únicamente al host mas próximo dentro del alcance de esta. No pueden ser usadas como dirección fuente en un paquete IPv6 y sólo pueden ser asignadas a routers configurados para un servicio anycast, los cuales poseen en sus tablas de enrutamiento los siguientes saltos y los host de destino si estos están ligados a los enlaces en sus interfaces; el envío dependerá de la topología y el estado de la red. El host que se encuentre mas accesible desde el punto de vista del emisor será el que reciba el paquete.

Las direcciones anycast no poseen prefijos ni estructura específicos. Dependerá de los diseñadores del servicio. En términos generales posee la siguiente forma, ver la *figura 1.3.*

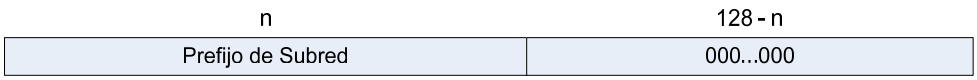


Figura 1.3 Dirección Anycast

El cabezal IPv6 posee una longitud fija de 40 bytes. Se diseñó para que sea más simple que su predecesor IPv4 en razón de mejorar el desempeño de los routers. Los campos de IPv4 retirados en IPv6 son: IHL, tipo de servicio, identificación, fragmentos, protocolo, suma de cabecera y opciones; sus funciones quedan relevadas a protocolos de capas superiores o a las *cabeceras de extensión*. Se observa en la *tabla 1.9* la cabecera IPv6

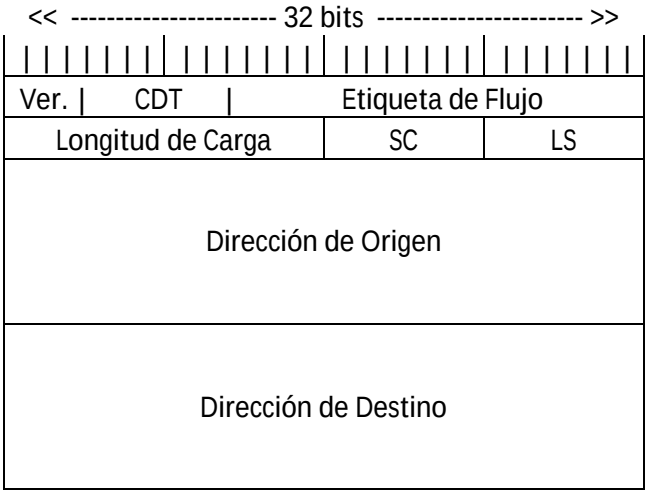


Tabla 1.9 Cabecera IPv6 [5]

El campo *Ver* v*ersión* indica que se trata de un paquete IPv6, *CDT (Clase De Tráfico)* es un indicador de prioridad, *Etiqueta de Flujo* es usada en funciones de QoS indicando a los routers que el paquete pertenece a una secuencia que debe tener un tratamiento especial, *Longitud de Carga* tamaño de los datos y las cabeceras de

extensión, LS *(Limite de Saltos)* número máximo de veces que puede ser reenviado por los routers. SC *(Siguiente Cabecera)* indica que tipo de cabecera viene a continuación, estas cabeceras son opcionales y cumplen funciones como fragmentación, seguridad, enrutamiento, movilidad entre otras. En la *figura 1.4* se observa un paquete IPv6.

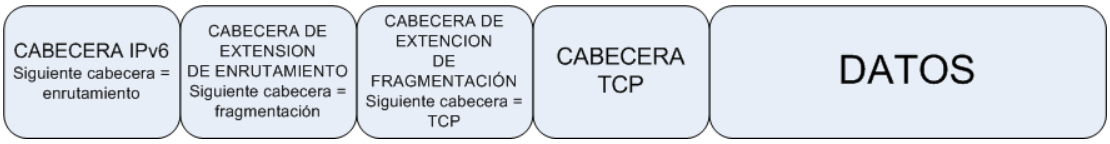


Figura 1.4 Paquete IPv6.

1.3.3.3 Protocolos de Estado del Enlace

OSPF *(Open Shortest Path First)* es el protocolo mas usado en internet, permite el balanceo de carga que transporta la red, tiene una métrica especial con la que cada router mide el ancho de banda de los enlaces conectados directamente a sus interfaces para luego compartir esa información con los routers vecinos en un área llamada AS *(Autonomous System)*, luego cada uno de ellos calcula las mejores vías para el enrutamiento de paquetes y actualizan o construyen sus tablas de enrutamiento, en función de los cambios de tráfico y topología de la red. Un ISP se puede considerar un AS.

La AS se encuentra dividida en *áreas*, estas se *inundan* periódicamente con mensajes OSPF en IP de broadcast emitidos por los routers para compartir la información. Todas las áreas están conectadas a una especial llamada *área 0.* Hay routers de borde que comparten información resumida entre dichas áreas.

La versión que soporta IPv6 es OSPFv3.

IS-IS *(Intermediate System to Intermediate System)* es un protocolo parecido al OSPF pero diseñado para redes de gran tamaño y con opciones abiertas para permitir la escalabilidad de la misma, Este no envía sus mensajes de enrutamiento en paquetes IP, para ello usa su propio direccionamiento especial. Los routers crean mapas de la topología de red que pueden alcanzar. Igual existen áreas pero ya no es necesaria una “área 0”

1.3.4 La capa de Enlace

Es igual que hablar de las capas 1 y 2 del modelo OSI; son los protocolos y hardware que se encargan de mover paquetes entre dos nodos pertenecientes a un mismo enlace en la internet. Es importante destacar que los protocolos de capas superiores le son transparentes, es decir IPv6 no afecta de ninguna manera el funcionamiento de esta capa. Existe una gran cantidad de protocolos y tecnologías, algunas como *frame relay* y *ATM (Asinchronous Transfer Mode)* aunque aun muy usadas se encuentran en proceso de eliminación.

1.3.4.1 Línea Digital del Abonado

Llamada comúnmente DSL *(Digital Subscriber Line)*, es un *acceso de última milla* o el último enlace entre la red de distribución y el abonado. Es la tecnología que permite el uso del par de cobre telefónico para transmitir señales digitales de banda ancha, hasta 40Mbps en las versiones mas recientes. Su principal limitación es la distancia, a mayores frecuencias de operación menor alcance. Fue diseñado para adaptar las líneas telefónicas de banda de voz a la transmisión de datos a altas frecuencia con el uso de métodos de modulación y codificación digitales, coexistiendo con la señal de voz analógica. Estas líneas se conectan a la red de distribución mediante un equipo llamado DSLAM *(Digital Subscriber Line Access Multiplexer)* el cual agrupa varias líneas DSL.

1.3.4.2 Metro Ethernet

Ethernet es un protocolo de acceso al medio, que a diferencia de los protocolos que trabajan en base a multiplexación para evitar colisiones entre las señales provenientes de dos o mas nodos que colocan datos en el medio, este protocolo las permite. Si un dispositivo debe colocar una trama en el medio, no esperará un turno o autorización para hacerlo, simplemente comienza a transmitir; si otro dispositivo se encuentra haciendo lo mismo entonces se producirá una colisión. Esta es detectada por las interfaces involucradas y detienen la transmisión, esperan entonces un tiempo aleatorio distinto cada una y retransmiten. Los switches evitan la incidencia de colisiones permitiendo que las redes sean más rápidas.

Metro ethernet es una implementación a nivel WAN, para redes de distribución masivas. Usa una configuración de red en forma de anillo y en la mayoría de los casos transmite a nivel L1 en fibra óptica mediante SONET *(Sinchronous Optical Networking)* o SDH *(Sinchronous Digital Hierarchy)* a velocidades de hasta 20Gbps.

1.4 Conmutación de Etiquetas de Multiprotocolo

MPLS *(Multiprotocol Label Switching)* es un protocolo que no se adapta al modelo OSI, se encuentra entre las capas 2 y 3 de este. No es L2 ya que va mas allá del vinculo y no es L3 ya que tiene solamente significado local, pero su gran ventaja es que permite transportar todo tipo de protocolos de capas 2 y 3 a través de una red. Mediante la agregación de *etiquetas* que representan rutas y sub-rutas llamadas LSP *(Label switch path)*, estas comienzan y terminan en routers LER *(Label Edge Router)* que se encuentran en los extremos de la red. Los routers intermedios son llamados LSR *(Label Switch router)*.

Los LER leen la dirección de capa 3 y etiquetan el paquete con la LSP que deben seguir. La elección y creación de estas rutas viene dada por la información obtenida a partir de los protocolos de enrutamiento como OSPF. Los LSR coordinan

sus acciones mediante el protocolo LDP *(Label distribution Protocol)* el cual consta de un conjunto de procedimientos y mensajes.

La implementación de MPLS permite la creación de diversas VPLS *(Virtual Private LAN Service)* las cuales son redes virtuales que pueden coexistir en una misma infraestructura física de red, en un ISP existiría una VPN por cada servicio, por ejemplo VoIP o IPtv, estas serían administradas de manera independiente e implementados en los LER. Otra ventaja es la reducción de la complejidad en los routers intermedios debido a que solo reenvían en función de lo que dice la etiqueta, todo el trabajo queda relegado a los routers de borde.

CAPÍTULO II
RED DE DATOS DE LA CANTV

2.1 Descripción de la Empresa

2.1.1 Historia

Esta compañía, conocida actualmente como CANTV fue fundada en 1930 en los últimos años del general Juan Vicente Gómez quien otorgara una concesión para la construcción de una red telefónica a nivel nacional a Félix Guerrero, quien era el accionista mayoritario de esta nueva empresa que ese mismo año compra las compañías telefónicas regionales como *Electrical Appliances Company Limited* que proveía servicios desde Caracas hasta Puerto Cabello.

En 1946 en la junta de gobierno se producen cambios en la administración pública de las telecomunicaciones y el estado contrata y administra sus propias redes de comunicaciones. Al hacer esto desarrolla una red que comienza a desplazar a CANTV como el principal proveedor de telefonía.

En 1958 con el objeto de expandir y modernizar la red nacional de telecomunicaciones el estado nacionaliza la CANTV al comprar la mayoría de las acciones de la misma, así como la compra del resto de compañías telefónicas privadas en el país, proceso que culmina en 1973.

En 1962 el ejecutivo nacional le asigna a CANTV la operación, administración y desarrollo de los servicios de telefonía local larga distancia, télex, radio, facsímil, teléfonos, transmisión de datos y otras facilidades para la transmisión de radio y televisión.

En 1990 el estado decide vender el 40% de las acciones a entes privados con el fin de actualizar la red, la cual acusaba de grandes retrasos. Después de una licitación internacional resulta como ganador el consorcio Venworld Telecom C.A.

Durante los primeros seis años como empresa privatizada es sometida a un profundo proceso de expansión y modernización de las redes de datos, voz, fijas y móviles, mediante la inversión de un capital de 3.000 millones de dólares. Se implementa la red ATM/frame relay y la digitalización de la plataforma de acceso. Se comienza la interconexión de las principales ciudades mediante fibra óptica y de la misma manera se realizan varias conexiones internacionales submarinas.

En 1996 se fortalece la privatización cuando el estado coloca en oferta publica el 34,8% del capital accionario, con lo cual comienza a cotizar en las bolsas de Nueva York y Caracas.

Entre 1998 y el 2000 ya como empresa de total administración privada se concreta la transformación de la estructura organizacional creándose nuevas unidades de negocios teniendo al cliente como nuevo enfoque estratégico. Nace también el producto de acceso comercial de banda ancha o ABA, el cual lidera hasta el día de hoy el acceso a internet a nivel de hogares.

Luego de la aprobación de la Ley Orgánica de Telecomunicaciones y el comienzo de la apertura total del mercado, entre los años 2000 y 2003 CANTV comienza la integración de las empresas del grupo.

Del 2004 al 2006 comienza un proceso agresivo de desarrollo de la redes de datos dada la alta demanda del sector, instalando puertos ABA en la mayoría de las centrales fijas. Para finales del 2006 CANTV cuenta con 467.000 usuarios de banda ancha.

El 21 de Mayo del 2007 el estado asume el control de la compañía luego de adquirir el 87% de sus acciones. Para el día de hoy es el principal proveedor de comunicaciones en Venezuela de manera directa o indirecta.

2.1.2 Visión

Ser el proveedor preferido de servicios integrales de comunicación en Venezuela, y satisfacer plenamente las necesidades específicas de sus clientes bajo excelentes patrones de ética y responsabilidad, mejorando la calidad de vida de los

venezolanos al proveer soluciones de comunicación que exceden las expectativas de nuestros clientes.

La empresa tiene los siguientes objetivos:

- Ampliar la cobertura geográfica, incluyendo a todos los segmentos de la población, ofreciendo tarifas justas y solidarias para promover una competencia más equitativa, con atención particular para cada segmento de la población para facilitar la integración al uso de las telecomunicaciones.
- Garantizar autonomía de la empresa: CANTV será eficiente en sus operaciones, de manera de generar los recursos requeridos para acometer proyectos con rentabilidad social, pero siempre asegurando la viabilidad económica de la empresa.
- Avanzar hacia la soberanía tecnológica: CANTV apoyará la implantación del software libre, cumpliendo con el decreto 3390 del Ministerio de Ciencia y Tecnología. Además, impulsará la apropiación tecnológica por parte de los ciudadanos, promoverá el desarrollo endógeno, respaldará la formación de talentos nacionales y promoverá la sustitución de importaciones.
- Apoyar la integración Nacional e Internacional: CANTV cobra una dimensión internacional, expandiendo las fronteras tecnológicas de la nación, bajo el lineamiento del acuerdo ALBA, el proyecto satelital VENESAT-1, que servirá para brindar apoyo a los programas sociales del estado y facilitar la transferencia tecnológica [6].

2.1.3 Misión

Ser la empresa estratégica del estado venezolano operadora y proveedora de soluciones integrales de telecomunicaciones e informática, corresponsable de la soberanía y transformación de la nación, que potencia el poder popular y la integración de la región, capaz de servir con calidad, eficiencia y eficacia, y con la participación de la sociedad venezolana, contribuyendo al bienestar social.[6]

2.1.4 Servicios CANTV

2.1.4.1 Conexión a Internet

Es el principal servicio de la corporación, este se entrega mediante la conexión ABA, para lo cual cada usuario adquiere vía DHCP un grupo de direcciones IP (que depende del tipo de servicio contratado) cada vez que establece conexión. Este servicio ofrece distintos anchos de banda para adaptarse a las necesidades del cliente, desde usuarios domésticos hasta oficinas de pequeñas empresas. La resolución de direcciones URL se realiza mediante servidores DNS propios, ya descritos anteriormente en este capítulo. También esta disponible un servicio de correo POP.

2.1.4.2 Interconexión WAN

Cualquier empresa puede interconectar las distintas LAN de sus locaciones corporativas mediante la red CANTV, mediante accesos a la Metro-Ethernet con grandes anchos de banda.

2.1.4.3 Voz Sobre IP

Permite la comunicación telefónica mediante el protocolo TCP/IP y gestionado por el protocolo SIP *(Session Initiation Protocol)* el cual admite a su vez la apertura de varios tipos de sesiones multimedia como video conferencias y videojuegos. VoIP permite llamadas a teléfonos PSTN y tiene alcance mundial.

2.1.4.4 Televisión Vía IP

Aún en desarrollo este servicio permitirá el acceso a canales de dos maneras distintas: en vivo mediante transmisión multicast y videos por demanda en tráfico unicast. Usará codificación de video comprimido MPEG4.

2.1.5 Tecnología

Dado el gran crecimiento de las redes de datos a nivel global CANTV ha venido implementando las *redes de siguiente generación* NGN *(Next Generation Networks)* las cuales son capases de ofrecer servicios *triple play* que constan de voz, acceso a internet en banda ancha y video, reconstruyendo toda red PSTN. Para esto la empresa ha unido esfuerzos con compañías de telecomunicaciones como Huawei, Ericsson, ZTE, Alcatel Lucent y Cisco Systems entre otras, para desarrollar un core y una red de acceso metro Ethernet, en coexistencia con los switches PSTN digitales (SS7) que representan inversiones con todavía muchos años de vida útil para considerar remplazarlos por sistemas de VoIP, en la *figura 2.1* se puede observar el esquema general del cambio de arquitectura de red.

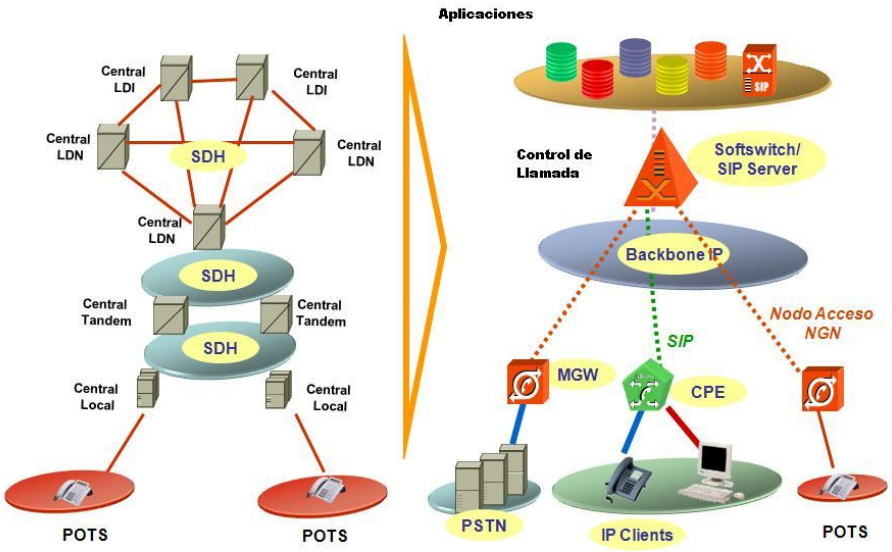


Figura 2.1 Migración NGN [7]

De la figura anterior, SIP es un manejador de abonados en la red de interfaz con Hewlett Packard Opencall para la tasación/facturación de servicios multimedia como VoIP entre otros. El *softswitch* actúa como un gestor en la interconexión de llamadas entre PSTN e IP. MGW *(Media Gateway)* es un convertidor de tráfico IP-TDM que permite la conexión con la red PSTN.

La red de datos de CANTV se puede dividir en dos bloque principales, el backbone y la red de acceso.

2.1.5.1 La Red de Acceso

Esta conformada por tecnologías L2 que son la red de transporte metro-ethernet o la ATM/frame relay y el acceso de última milla. Este último ofrece servicios de conexión a internet por ABA *(Acceso Banda Ancha)* y VoIP, mediante un CPE *(Costumer Premise Equipement)* que es la interfaz de usuario para estos. VoIP requiere un ATA *(Analog Telephone Adapter)* en el caso de usarse un equipo de teléfono puramente POTS *(Plain Old Telephone System)* el cual se puede conectar a la red PSTN con el uso de filtros pasivos pasa-bajo que separan la señal de datos de la

de voz. El transporte a través de la línea de abonado (par de cobre telefónico) es mediante DSL, mas específicamente ADSL *(Asymmetric Digital Subscriber Line)* que permite anchos de banda gestionables desde los 1,5 hasta los 12 Mbit/s [8] en downstream y desde 0,5 hasta 1,3 Mbit/s en upstream. Esta tecnología usa ATM como protocolo L2 en la conexión punto a punto CPE a DSLAM *(Digital Subscriber Line Access Multiplexer)*. Este último añade el tráfico de un grupo de subscriptores a la red metro-ethernet; previamente estas líneas traviesan por un regleta de filtros que dividen la señal analógica de voz de la datos. Actualmente se encuentra desarrollando un nuevo modelo como el que se muestra a continuación en la *figura 2.2*

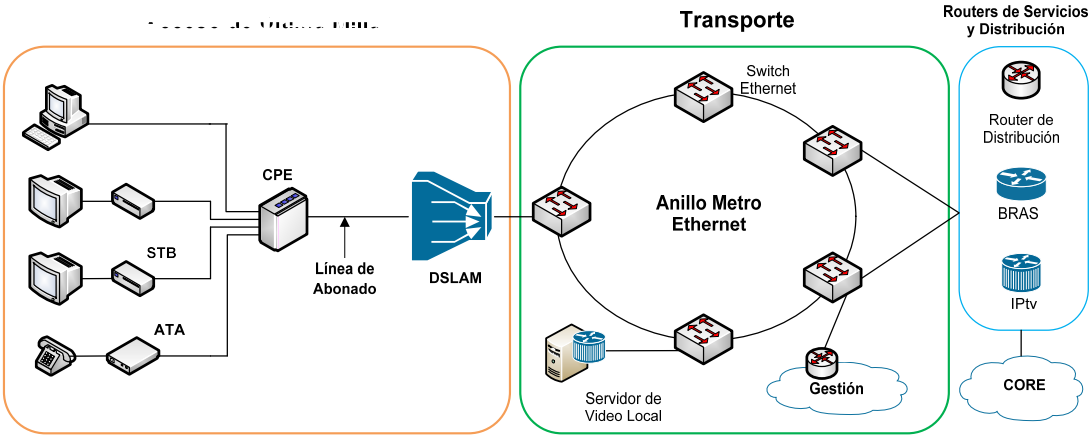


Figura 2.2 Red de Acceso. Fuente: Autor

En esta nueva configuración se añade el servicio de IPtv, mediante el cual se pueden conectar televisores estándar a la red interna (4 puertos ethernet) proveniente del CPE mediante el STP *(Set Top Box)*. El enlace con el DSLAM será ahora mediante ADSL2+ con 24 Mbit/s de downstream y 1 Mbit/s de upstream (en algunas regiones ya existe este servicio DSL) [7].

En un aproximado del 70%, los equipos DSLAM son de la familia Alcatel-Lucent 7300/7301 ASAM *(Advansed Services Access Manager)* y 7302 ISAM *(Intelligent Services Access Manager)*, estos poseen desde 120 hasta 2304 líneas por rack, divididas en tarjetas desmontables. Estos se pueden conectar al switch ethernet

en diversas topologías como estrella, anillo y cascada. Otro 30% lo cubren equipos Ericsson , ZTE y Huawei.

Los routers de servicios se encuentran entre los routers de distribución del backbone y los anillos metro-ethernet. Los routers BRAS *(Broadband Remote Access)* dirigen tráfico de internet para el servicio ABA; en estos recaen funciones de QoS y gestión de abonado para las diferentes modalidades del servicio, se trata de routers Juniper ERX y E320. Por último están los routers para el tráfico de video IPtv, estos son Cisco 7609.

La red de transporte ATM/frame relay se usa para interconectar diversas LAN privadas geográficamente distantes pertenecientes a clientes corporativos. Aunque aún existe una cantidad importante de estas redes, CANTV no promueve mas estas tecnologías, actualmente se implementan VPLS *(Virtual Private LAN Sertvice)* mediante la red metroethernet y accesos ABA.

La red metro-ethernet está conformada por 30 anillos interconectados entre ellos por switches y por los routers de distribución, manteniendo así una estructura de comunicaciones redundante, con diferentes velocidades que van desde 1Gbps hasta los 20Gbps. Las conexiones se realizan mediante enlaces de fibra óptica, exceptuando algunas extensiones tipo stub (un solo acceso) en que se usan radio enlaces. En la *figura 2.3* se puede observar un ejemplo de la distribución de estos anillos.

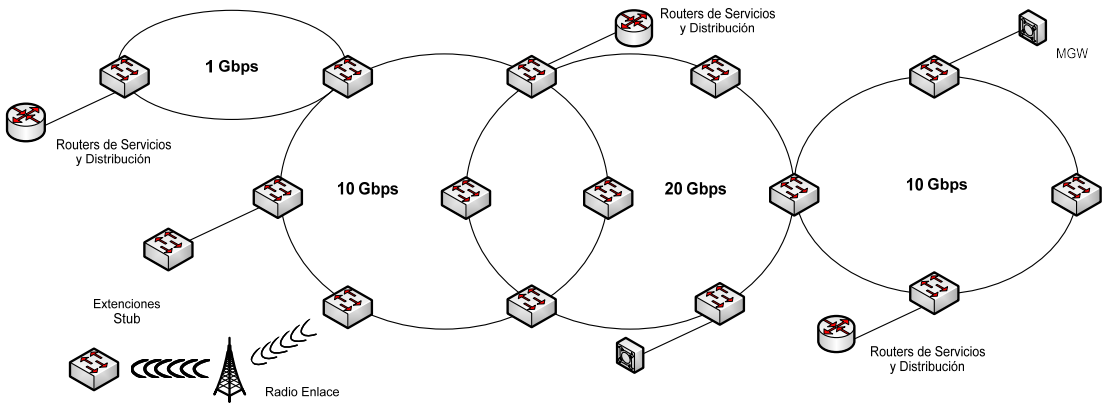


Figura 2.3 Anillos Metro-ethernet. Fuente: Autor

A estos anillos se conectan los equipos MGW *(Media Gateway)* que permiten la agregación de tráfico de voz PSTN a la red (convertidor IP – TDM), permitiendo la interconexión de las centrales telefónicas con equipos Huawei UM8900 y la conexión directa de líneas POTS mediante los equipos Huawei UA5000.

En los switches se conectarán también en un futuro cercano dispositivos de broadcasting WiMax, para ofrecer conexión banda ancha móvil a la internet.

En esta sección de la red el enrutamiento se realiza a partir de las direcciones L2 o MAC de los dispositivos conectados. A diferencia de una red LAN ethernet común, en esta topología se pueden encontrar gran cantidad de enlaces redundantes, por lo que se cuenta con STP *(Spanning Tree Protocol)*, este evita la formación de bucles permitiendo un solo camino activo a la vez entre dos dispositivos y mantiene los redundantes en reserva para el caso de fallas. Se adapta a los cambios en la topología reconfigurando los switch de manera de asegurar una conectividad optima, para esto el protocolo usa mensajes de comunicación llamados BPDU *(Bridge Protocol Data Units)*. STP realiza el trabajo para L2 que protocolos como OSPF hacen para L3.

Aunque estos switches enrutan mensajes puramente en L2, también poseen direcciones IP de L3 usadas para su gestión y algunos servicios, por lo que son capaces de escuchar mensajes OSPF y responder a ellos. Sin embargo un mensaje entrante a una interfaz cuya dirección MAC de destino no sea la propia de esta misma, será enrutado sin leer la cabecera de capa superior.

A algunos de estos anillos de nivel regional se les añaden plataformas de gestión de los mismos; también se pueden encontrar servidores de video por demanda VoD *(Video on Demand)* de carácter local.

Los switch metro-Ethernet de CANTV son equipos Alcatel-Lucent 7450 ESS, los cuales tienen interfaces de 10/100/1000 Ethernet sobre cualquier medio.

2.1.5.2 El Backbone

Es el corazón de la red que interconecta todos los servicios y el borde de internet con la red de acceso. Se puede apreciar en la *figura 2.4*

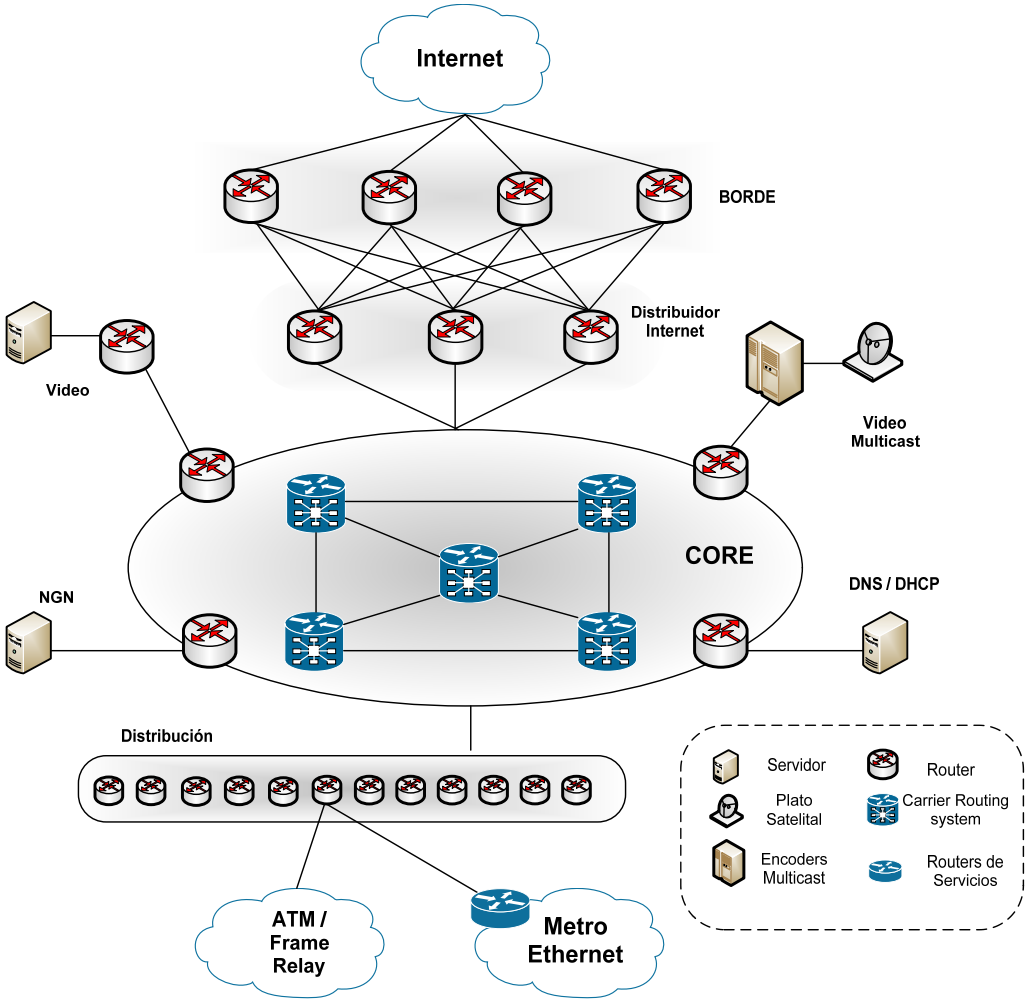


Figura 2.4 Backbone. Fuente: Autor

Esta conformado principalmente por los siguientes routers Cisco:

- *Crs8* es un *carrier router system* o router de carga para tráfico de backbone, posee slots para interfaces de línea de 40Gbps cada uno, a full

carga puede manejar una carga de 92Tbps. Se encuentran únicamente en el core.

- *12410* de la familia 1200 es un router diseñado como proveedor de IP/MPLS, es conocido también como GSR *(Gigabit Switch Router)*, tiene una capacidad de conmutación que va desde 200 hasta 800 Gbps. Se encuentra ubicado en el borde de distribución, internet, distribución de internet y core.
- *7609* de la serie 7600 es también un proveedor de servicios IP/MPLS, con una capacidad de conmutación de hasta 720 Gbps en una configuración de slots de 40 Gbps cada uno. Se encuentran ubicados en el borde de internet, en el borde de los servicios con el core y en la agregación de VoD a nivel regional directamente a la metro-Ethernet.

Estos se encuentran interconectados por diversas líneas de transmisión como *STM-64 POS* de 9954 Mbps sobre protocolo SONET, además de *1 Gigabit Ethernet* (1GbE) y *10 Gigabit Ethernet* (10GbE), con velocidades de 1 y 10 Gbps respectivamente.

Los diversos routers usan el sistema operativo IOS *(Internetwork Operating System)* cuya interfaz con el operador o CLI *(Command Line Interfase)* permite el acceso a la configuración de los mismos, entre otras funciones la asignación de nombres y direcciones estáticas a las interfaces, servicios como MPLS, VLAN *(Virtual LAN)*, VPLS, QoS, obtención de direcciones dinámicas, relevación DHCP, NAT *(Network Address Translation)*. Este sistema operativo se encuentra alojado junto con su configuración en dispositivos de memoria flash que permiten un rápido arranque del mismo mientras que las tablas de enrutamiento son escritas en memoria RAM. A este sistema se puede acceder de varias maneras, mediante un cable de consola (par de cobre) el cual es la única manera de realizar la configuración inicial del equipo; una vez realizada se le puede acceder remotamente mediante el uso de los protocolos Telnet *(Telecommunication Network)* o SSH *(Secure Shell)* los cuales alcanzan el dispositivo mediante la dirección IP de una de sus interfaces.

Una red MPLS cubre todo el back-bone, los routers LER son aquellos que conforman la red de distribución (junto con los routers de servicios), borde de internet y acceso de los servicios al core. El protocolo de enrutamiento es OSPFv2, el cual posee 10 zonas, siendo la zona 0 el backbone.

Los servidores de video multicast están conformados por los *encoder multicast* los cuales convierten señales de tv en vivo (obtenida a través de las antenas de Camatagua), en formato MPEG-4 para luego ser agregados al core a manera de paquetes IP de multicasting. Además están los servidores de VoD *(Video on Demand)* para servicios de video unicast por solicitud.

Los servidores NGN están conformados por los servidores SIP para administrar principalmente los servicios de VoIP junto con el SBC *(Session Border Control)* y el OCMP *(Open Call Media Plataform)*. El Softswitch interactúa con la red PSTN controlando el enrutamiento de este tráfico y su respectiva señalización.

Los servidores DNS están conformados por equipos de arquitectura x86 con sistemas operativos Microsoft Windows 2000 Server. Las funciones DNS son realizadas por el software BIND *(Berkeley Internet Name Domain)* de versión 9.4.2. El primero de ellos es el SOA *(Start Of Authority)* el cual registra todas las direcciones autoritativas para los dominios de red de la corporación. A este acceden el servidor de *navegación* con las direcciones asociadas a las redes internas, el servidor *data center* el cual resuelve direcciones de los diversos servidores internos; estos dos mencionados anteriormente sólo son alcanzables por host internos de la red, no por internet ni por los clientes. El último de ellos es el *dinámico* que se usa para la navegación de internet de los clientes, contiene los registros públicos del SOA pero como no autoritativos, así como comparte registros con otros servidores DNS fuera de la red.

Los servidores DHCP también son x86, usan el sistema operativo Advan Server 4 el cual es una distribución Linux. Existen solo 4 servidores los cuales están en Caracas y 4 como back-up de los primeros en Barquisimeto. El software usado para la aplicación es el CNR *(Cisco Network Registrar)* versión 6.2.3.

El acceso a internet, la “nube” en la *figura 2.4* antes referida, es un conjunto de enlaces, principalmente por fibras ópticas (mayoritariamente submarinas) con otros ISP y redes en el mundo. Estas conexiones son alquiladas a las compañías Global Crossing, Sprint, France Telecom, MCI, Telefónica y LANautilus, en la *figura 2.5* se puede apreciar la red mundial de la primera. Estas redes se interconectan unas con otras logrando el alcance mundial.

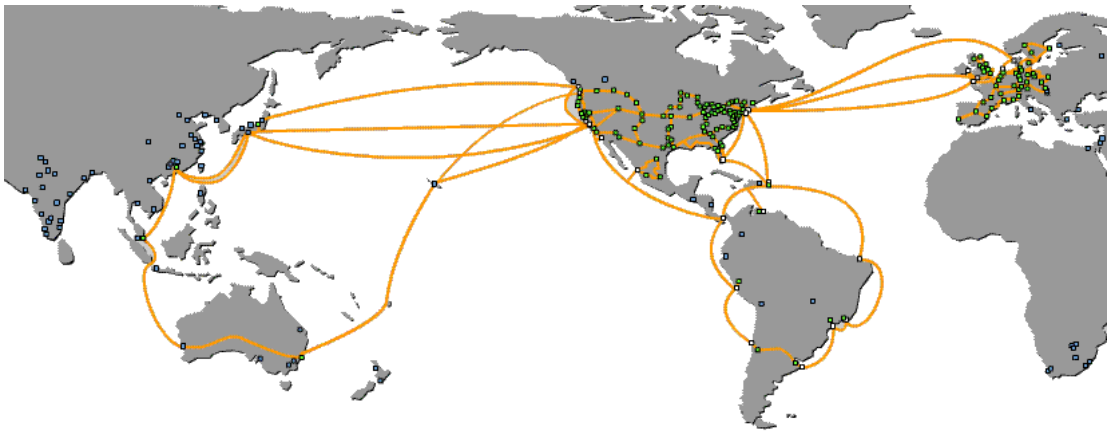


Figura 2.5 Red Global Crossing [9]

Estas redes están sujetas al protocolo BGP para el enrutamiento de datagramas entre los routers de borde de internet de los distintos ISP o redes privadas que se encuentran conectados a ellas.

CAPÍTULO III

MOTIVOS PARA EL DESPLIEGUE DE IPv6 Y EFECTO EN LOS SERVICIOS CANTV

3.1 IPv6 frente a IPv4 en la Red CANTV

Existe una variedad de argumentos técnicos en pro de la implementación de IPv6. Una breve descripción indicará cuáles de estos representan mejoras sustanciales con respecto a IPv4 para que la migración de protocolo se vea justificada.

La cabecera IPv6 al poseer menos campos, delegando funciones como fraccionamiento a los dispositivos de origen y destino, así como a capas superiores, además de una longitud fija de 40 bytes en realidad representa una menor carga de procesamiento y uso de memoria para los routers. Sin embargo en los últimos años se pueden ver procesadores cada vez mas poderosos en los routers; los usados por la corporación no presentan problemas de sobrecarga ni están cercanos a ellos, la velocidad de la red está limitada por los medios y el acceso a ellos. Esta característica del protocolo no representa una motivación para la migración.

El soporte para aplicaciones en tiempo real dado por el campo flow label de la cabecera IPv6 permite la aplicación de QoS, servicios multimedia como un stream de video cuyos paquetes IPv6 que los conforman quedan identificados como parte de un mismo flujo siendo entonces tratados de la misma manera y con la misma prioridad por los routers que atraviesan. La red IP de CANTV funciona bajo el protocolo de etiquetas MPLS, el cual cumple la misma función y la cabecera IP es ignorada por los routers LSR intermedios, por lo que para los intereses de CANTV esta función carece de importancia.

En IPv6 mediante cabeceras de extensión se brinda seguridad aplicando autentificación de fuente y encriptación; IPv4 cuenta con IPsec que opera de la misma manera garantizando las mismas condiciones de seguridad. Además hoy en día los

flujos de información crítica como son los de gestión de red usan protocolos de seguridad de capas superiores como SSH. Aunque IPv6 presenta mejoras de seguridad, no representa un motivo suficiente para el cambio.

La cabecera de extensión de movilidad en IPv6 permite a dispositivos móviles obtener una dirección “prestada” cuando se encuentran en redes distintas a su red original, entre tanto los paquetes dirigidos a la dirección de origen son redirigidos hacia la red foránea donde el dispositivo móvil se encuentra conectado. IPv4 cuenta con el protocolo *mobileIP* que realiza las mismas funciones aunque de distinta manera. Esta característica no se puede considerar como una mejora sustancial del protocolo, por lo que tampoco se puede considerar como un estímulo a la migración.

Cuando un dispositivo IPv6 se conecta a una red, este puede obtener su propia dirección IP usando la dirección MAC como la *interface ID* y obtiene el prefijo de red preguntándolo a algún router que se encuentre conectado, mediante el procedimiento *autodiscovery;*, si no hay routers conectados los host toman como prefijo de red el de link-local. IPv6 es entonces un protocolo *plug and play*, esta es una característica que IPv4 no posee y que es beneficiosa en redes pequeñas; sin embargo, a CANTV le interesa mantener el control de las conexiones a la red y las direcciones asignadas usando servidores DHCP. Este entonces no es un motivo para el cambio de protocolo.

IPv6 posee 128 bits en los campos de dirección, proveen una capacidad de direccionamiento muy superior a la que IPv4 puede ofrecer con 32 bits. Esta razón es la que convierte al protocolo en un requisito necesario para CANTV además de todos los ISP y organizaciones que conforman la World Wide Web, dado el agotamiento al que se ve sometido actualmente el stack de direcciones no asignadas de IPv4.

3.2 Agotamiento de las Direcciones IPv4

La IANA es la organización internacional encargada de la administración de los aspectos relacionados con internet, entre ellos la asignación de los bloques o *pools* de direcciones IP. Para esto divide la cantidad total de estos por zonas donde las organizaciones regionales las asignan a cada país. LACNIC *(Latin American and Caribbian Internet Adresses Registry)* es la responsable de la región donde está Venezuela.

Actualmente ya casi no quedan bloques IPv4 libres y se estima que para el 2011 estos se habrán acabado. De allí el principal motivo para la implementación de un protocolo de direccionamiento con capacidades más amplias, como IPv6. En la *figura 3.1* se aprecia la tendencia al agotamiento de direcciones IPv4 por año desde 1999, en bloques /8 equivalentes a 1/256 del total de direcciones (/8=2^{24}= 16777216).

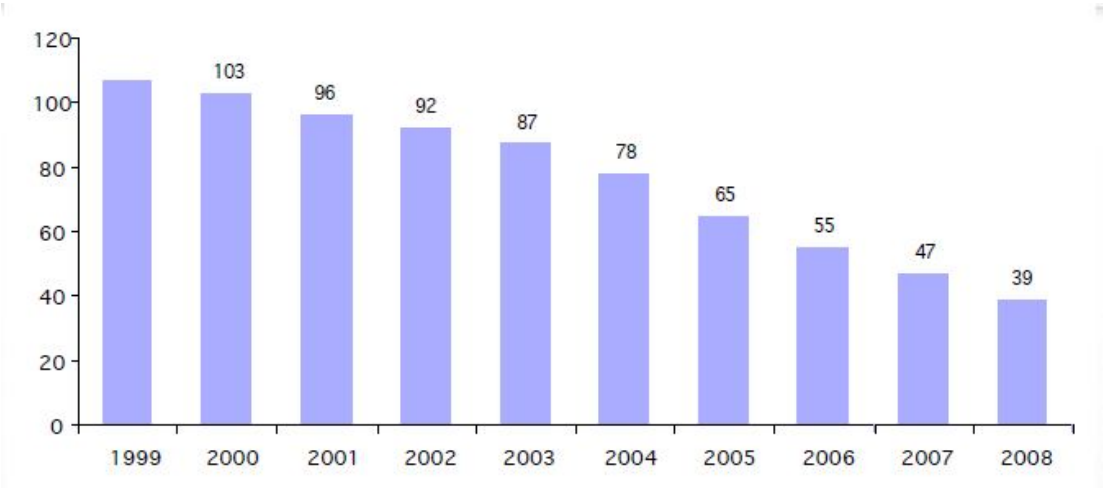


Figura 3.1 Stock IPv4 de la IANA [10]

Se observa que desde 1999 la expansión de las redes y nuevos dispositivos conectados a internet (automóviles, consolas de videojuegos, electrodomésticos entre otros) han crecido de manera acelerada, así como los sistemas *always on* que nunca se

desconectan impidiendo la relevación de su dirección IP. Existen técnicas como NAT que permiten a clientes de un ISP tener conectividad a internet para su LAN teniendo configurados sus host con direcciones privadas mientras se usan una o algunas pocas direcciones públicas, lo que implica un ahorro sustancial de estas, para lo cual el router de borde de esta red sustituye las direcciones privadas de un grupo de hosts por una sola dirección pública, permitiendo que los routers del ISP reenvíen sus mensajes, para reconocer luego el host de origen se usan números de puerto de L4. Sin embargo esta técnica no ofrece conectividad total extremo a extremo, solo un acceso al internet que no permite a los hosts remotos reconocer de manera eficaz a los dispositivos de origen por lo que varios servicios no pueden funcionar de manera correcta.

Las acciones tomadas por la IANA incluyen la recuperación de bloques de direcciones asignados a organizaciones que por diversos motivos nunca alcanzaron a funcionar o sencillamente no los usaron ni tienen planes de expansión inmediatos.

Con IPv6 se cuenta con unas 340 sextillones de direcciones. LACNIC asigna bloques /32 (a menos que se requiera de tamaño superior), entonces con cada bloque se pueden crear 65536 subredes. Si se usa todo el campo site ID para crear nuevas sub-redes de menor jerarquía se obtienen otras 65536 de estas, entonces para cada una de las últimas tenemos $1{,}8x10^{19}$ direcciones posibles. Si consideramos la población de Venezuela en unos 30 millones de habitantes, cada uno podría disponer de 614.891.469.123 direcciones.

3.3 Antecedentes de IPv6

Actualmente existe un gran número de redes IPv6, la mayoría de carácter experimental y algunas que ya operan a nivel comercial, entre ellas: 6ren, 6init, 6tap, Freenet, WIDE, US Navy. De todas la mas notable es la 6bone, la cual fue la primera red IPv6. Comenzó sus operaciones en 1996 un año antes de que se publicó el RFC-2460, el cual definía finalmente al protocolo. Fue la mayor de todas las redes experimentales hasta el año 2006 cuando fue finalizado el proyecto.

Para Diciembre del año 2008, se cuentaba con 631 Sistemas Autónomos, 15518 routers y 109658 links [11], distribuidos de la siguiente forma en la *figura 3.2*.

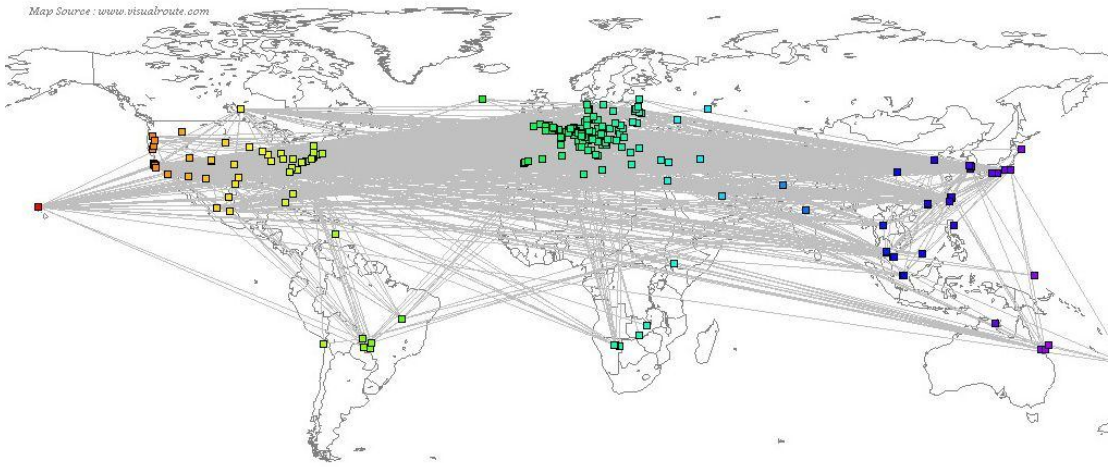


Figura 3.2 Despliegue de IPv6 [11]

Se puede observar que en Europa, USA y Asia se encuentran la mayor parte de ASs IPv6. En Latinoamérica solo México, República Dominicana, Brasil, Paraguay y Chile tienen desarrollos operativos de IPv6.

En Venezuela el único avance en IPv6 ha sido dado por la red REACCIUN *(Red Académica de Centros de Investigación y Universidades Nacionales)* la cual forma parte de *internet2*, una red mundial de alta velocidad con fines académicos y de

investigación. Este avance sin embargo no se puede interpretar como una red IPv6 sino como una red IPv4 con alcance a redes IPv6 mediante el uso de *túneles*, que permiten enmascarar paquetes IPv6 con cabeceras IPv4 permitiendo así ser encaminados a través de redes comunes.

La corporación CANTV conociendo la situación del agotamiento de las direcciones IPv4 y dados sus planes de expansión y nuevos servicios, ha comenzado el camino a la migración hacia IPv6 para poder así brindar conectividad total a la nueva internet que vendrá de manera inevitable como solución al problema de direccionamiento mundial. Esta migración deberá ser lo más transparente posible al usuario y en convivencia con el protocolo IPv4 el cual tendrá validez por muchos años mas.

3.4 Puntos Críticos de la Red

El principal elemento afectado es el backbone, más específicamente los router en los bordes del mismo. Estos son los LER de la MPLS los cuales crean las rutas que deben seguir los paquetes, etiquetándolos, luego los router internos para poder encaminar estos paquetes interpretan las etiquetas sin leer las direcciones IP o la cabecera del protocolo al que pertenezca el paquete, debe recordarse que MPLS se trata de una tecnología multiprotocolo.

Por otra parte para que los LER puedan etiquetar paquetes IPv6 y por lo tanto construir LSPs para ellos, los routers deben operar con por lo menos un protocolo de enrutamiento que determine el estado de conectividad entre ellos. Actualmente se usa OSPFv2 el cual no es compatible con IPv6. Se hace necesario realizar una actualización de software en algunos routers del backbone para configurarlos con OSPFv3 el cual es esencialmente igual a su predecesor pero con soporte IPv6. Para los routers Cisco la versión de IOS que soporta este protocolo en los routers del backbone es la 12.3(11)T (o superior) y la 12.2S RLS3 (o superior) para los routers Cisco 7609, para los Juniper seria JunOS 6.2 (o superior). A nivel de hardware no se

requiere de ningún tipo de cambio en el backbone. Otra opción sería implementar IS-IS el cual requiere las mismas actualizaciones antes nombradas, la principal diferencia con OSPFv3 es que soporta una mayor cantidad de routers por área y sería apropiado en caso de un eventual aumento del tamaño del backbone.

La red de acceso cuenta sólo con dispositivos L2, switches y DSLAMs, que enrutan los paquetes en base a la dirección MAC ubicada en la cabecera ethernet, el protocolo de enrutamiento en la red metro-Ethernet es *spanning tree* el cual es puramente L2, por lo que la transmisión de paquetes IPv6 o IPv4 le es indiferente.

Los switches y DSLAMs poseen direcciones IP para configuración y para su uso en servicios como IPtv de multicasting. Estas son direcciones privadas por lo que no representan un gasto de recursos de direccionamiento y recordando que IPv4 coexistirá con IPv6 durante muchos años, no se requiere entonces de ningún tipo de cambio en este sentido para estos dispositivos, a menos que se requiera implementar multicasting en IPv6.

Actualmente la mayoría de los sistemas operativos que usan los host soportan IPv6 entre estos los mas usados: Linux, Solaris, Mac OS, OpenBSD, Windows 2000 y XP mediante opción de instalación o actualización, Windows Vista lo tiene de forma nativa. En el caso de Windows XP (service pack 1 o superior) el protocolo se puede implementar usando la opción “instalar” en “propiedades de conexión área local” o “propiedades de conexiones inalámbricas” y escogiendo “TCP/IP versión 6”.

Las diferentes compañías que brindan el acceso internacional a la red CANTV ya tienen conectividad IPv6 mediante sus propias MPLS. Los routers de borde de internet deben tener como EGP al protocolo BGPv4 el cual se encuentra soportado en las actualizaciones antes descritas para routers Cisco.

3.5 Operación de los Servicios CANTV bajo IPv4/v6

3.5.1 Conexión a Internet

Se debe garantizar el acceso a redes comerciales IPv4/v6. Aunque actualmente la mayoría de las redes son v4, ya existen numerosas redes v6 o v4/v6 que ofrecen diferentes servicios y aplicaciones; se les llaman *islas IPv6* y se espera que en un futuro cercano se revierta la situación, siendo las redes v4 las que sean minoritarias. El acceso a estas redes v6 se dará cuando el backbone esté preparado para encaminar datagramas IPv6 y los servidores DHCP y DNS puedan cumplir con sus funciones usando el nuevo esquema de direccionamiento en conjunto con el actual.

Los servidores DHCP actualmente no son capaces de suministrar direcciones IPv6 dinámicas a los clientes, ya que no manejan el protocolo DHCPv6, el cual es nativo de CNR versión 7.0.1 (o superior), programa de licencia Cisco Systems, por lo que se requerirá de realizar una actualización. Esta actualización permite entre otras cosas la clasificación de clientes según el tipo de servicio de conexión y la actualización de los registros DNSv6 en el servidor DNS de la zona local en el momento en que estos adquieren, renuevan o liberan direcciones. Los servidores DNS usan la aplicación BIND 9.4.2 la cual soporta registros AAAA permitiendo la resolución de URLs pertenecientes a aplicaciones IPv6.

3.5.2 Interconexión WAN

El objetivo es mantener una conectividad confiable entre las distintas LANs de los clientes corporativos, sin importar el protocolo L3 que usen en estas. La solución es la creación de diversas VPLS que mantengan conectadas a manera de una red virtual los diversos routers borde de las LANs privadas o CE *(Costumer Edge)*, los cuales a su vez se conectan vía metro ethernet con un router de distribución o servicio específicos o PE *(Provider Edge)*. En estos últimos se configuran rutas a

través del backbone mediante MPLS conectándose con otros PE implicados. MPLS es un transporte multiprotocolo por lo que puede llevar tramas ethernet que a su vez carguen con paquetes IPv4/v6. De esta manera se obtiene la conectividad deseada sin necesidad de que el cliente se vea forzado a realizar migraciones, a no ser que este último decida que CANTV gestione su nueva red, en cuyo caso se le deberán asignar un grupo de direcciones IPv6. En la *figura 3.3* se observa un ejemplo de interconexión WAN.

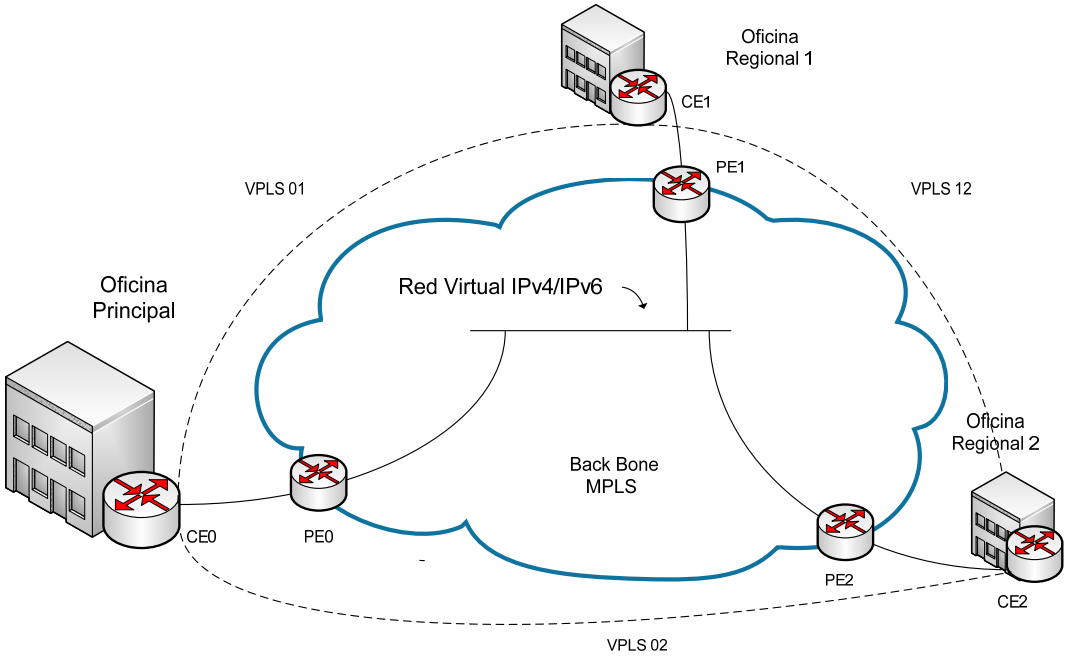


Figura 3.3 Interconexión WAN. Fuente: Autor

3.5.3 Voz Sobre IP

Este servicio de telefonía se encuentra disponible por los momentos solamente para los usuarios de ABA, en la *figura 3.4* se pueden observar sus componentes.

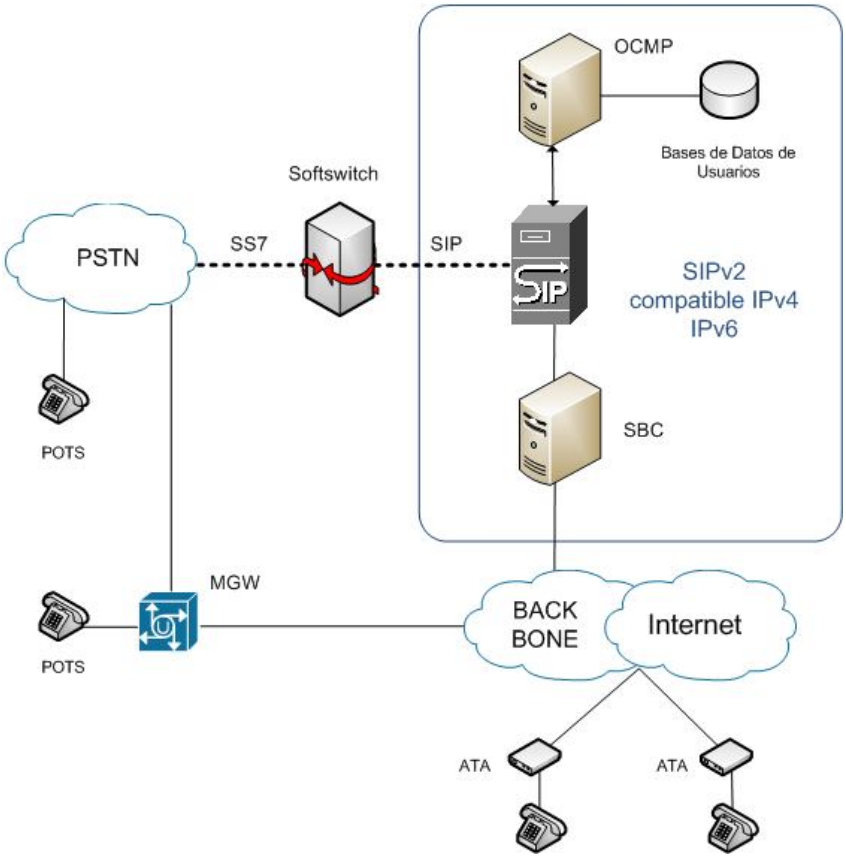


Figura 3.4 Voz Sobre IP. Fuente: Autor

En la base de datos conectada al OCMP marca Hewlett Packard se registran los usuarios (por su dirección MAC del ATA) asociados a una dirección IP obtenida vía DHCP, el servidor Siemens SIP gestiona el establecimiento de la conexión cuando un usuario VoIP o PSTN realiza una llamada. Todo el procedimiento es administrado por el OCMP que cumple funciones como autentificación y localización de usuarios y facturación, la comunicación con el medio PSTN se realiza a través del softswitch marca Siemens el cual funciona como una interfaz de señalización SS7 y SIP. Una vez establecida la conexión, la señalización de la misma queda a cargo del servidor Acme Packet SBC mientras que la señal de voz paquetizada viajaría directamente entre los dispositivos vía back-bone internet.

Los dispositivos antes mencionados así como el equipo ATA (Handy Tone 486) usado hasta ahora por los abonados, ejecutan de manera nativa el protocolo SIPv2, el cual esta descrito en el RFC 3261, en el que se establece la compatibilidad con IPv6 y la coexistencia de este con IPv4. Este servicio sólo requiere de ser configurado para poder ejecutarse en redes IPv4/v6.

El beneficio de usar IPv6 recae en el direccionamiento ilimitado de abonados, a los que se les podrían ofrecer mayor cantidad de líneas VoIP por servicio ABA, siendo otros factores como la capacidad de tráfico los únicos que limiten la prestación del servicio.

3.5.4 Televisión vía IP

Este servicio cuenta con dos modalidades de tráfico, unicast para VoD y multicast para video en vivo desde el *headend* ubicado en Camatagua. El direccionamiento para ambos vendrá dado por servidores DHCP exclusivos para este servicio y las direcciones IPv4 otorgadas por estos serán del tipo privado. Con esto se crea una cadena de televisión interna a la red CANTV. La aplicación de IPv6 solo aportará una capacidad de direccionamiento prácticamente infinita y si en lugar de usar direcciones site-local (equivalentes a IPv4 privadas) se usan global unicast y multicast con alcance global, se podrá tener acceso a futuros de servicios de televisión foráneos a la corporación.

Para servicio unicast se crea una VPLS por cada switch metro-ethernet, y a cada una de estas se les asigna un pool de direcciones privadas.

Para el servicio multicast también se crea una VPLS por cada switch de la red metro-ethernet y se asignan direcciones multicast IPv4 creándose así diversos grupos, uno por cada canal. Para el funcionamiento de este tipo de tráfico se ejecutarán dos protocolos distintos, el primero de ellos es PIM-SM *(Protocol Independent Multicast – Sparse Mode)*. Este no depende de el protocolo de ruteo unicast y se le llama de modo escaso ya que es aplicable en redes donde muy pocos hosts se encuentren subscritos a grupos multicast, a diferencia de versiones anteriores del protocolo. Este

construye las rutas a seguir para los paquetes multicast desde el emisor hasta el router final de servicio. El otro protocolo es IGMPv2/v3 snooping *(Internet Group Management Protocol)*; este funciona a nivel de la metro-ethernet. Cuando algún STB solicita ser agregado a un grupo multicast especifico éste envía una advertencia a su respectivo switch el cual solicita al router de servicio que se le envíe el trafico multicast solicitado; luego realiza el proceso inverso cuando detecta que no hay *oyentes* para un grupo dado.

Para aplicar IPv6 se deben configurar en los switches alguno de los dos protocolos MLD v1 o v2 *(Multicast Listener Discovery)* los cuales cumplen con las mismas funciones de IGMP v2 o v3 respectivamente, además en por lo menos una de las interfaces de los switches debe establecerse una dirección IPv6 (unicast) junto con la dirección IPv4 que ya posee. Los equipos Alcatel-Lucent 7450 ESS tienen estas capacidades al estar operando con la versión 5.0 de su sistema operativo y solo requerirán de ser configurados. En la *figura 3.4* se puede observar la distribución del servicio de televisión Multicast.

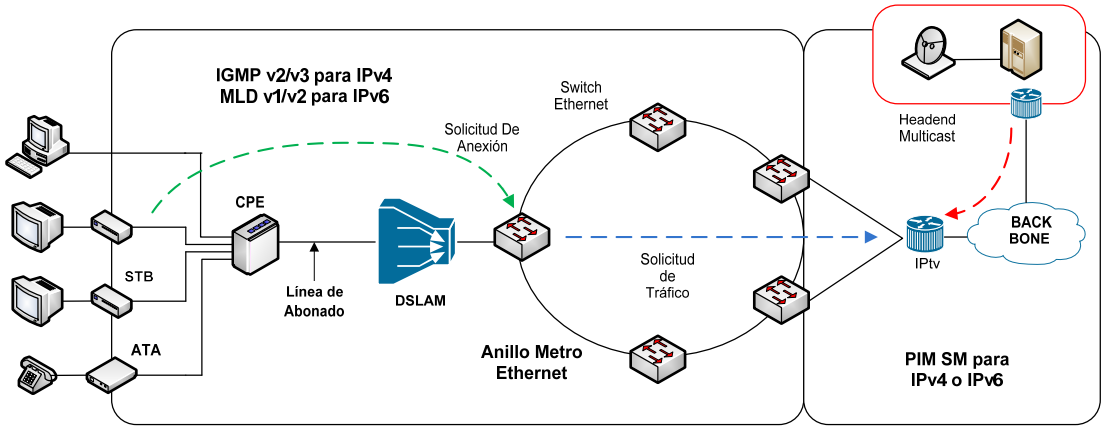


Figura 3.5 Servicio de Televisión Multicast. Fuente: Autor

CAPÍTULO IV

PROCESO DE IMPLANTACIÓN DEL PROTOCOLO DE DIRECCIONAMIENTO IPv6 EN LA RED DE DATOS CANTV

4.1 Áreas de Atención y Riesgos

Los protocolos IPv4 e IPv6 funcionan de la misma manera, en el sentido de que las funciones de ruteo se ejecutan de la misma forma mediante la construcción y consulta de tablas de enrutamiento en los routers, solo que IPv6 posee direcciones más extensas, este aspecto minimiza los riesgos y facilita la transición. Sin embargo estos protocolos son diferentes e incompatibles entre sí, la gestión de L3 para redes v4/v6 se debe realizar de manera separada para IPv4 e IPv6 e independiente uno del otro, lo que implica para la corporación un aumento en los costos.

Las diferencias entre ambos protocolos son lo suficientemente vastas como para que exista la necesidad de re entrenar al personal de gestión de red, el cual está acostumbrado a trabajar con un protocolo IP con mas de 20 años siendo el más robusto método L3 de comunicación paquetizada. QoS, MIP *(Movile IP)*, IPsec, fragmentación e ICMP están entre las características comunes a ambos protocolos pero que funcionan de manera distinta, además de la diferencia en el modo de direccionar los 128 bits de IPv6 mediante prefijos y los 32 bits de IPv4 mediante mascaras de subred. En CANTV, donde no se requerirán de cambios de hardware, el costo de entrenamiento podría llegar a ser el mas notorio de los gastos de migración.

Según un estudio [12] realizado por una sólida empresa proveedora de seguridad en redes, Arbor Networks, la mayoría de los ISP en los Estados Unidos temen que se presenten nuevos y mas complejos problemas de seguridad a medida que se despliegue el nuevo protocolo; esto es debido a la falta de experiencia que en general se tiene del uso comercial del mismo por lo que se supone la existencia de

agujeros de seguridad desconocidos en éste, Tomando en consideración que aún en IPv4 se observan nuevos ataques a nivel L3, es de esperarse que con IPv6 usuarios de red con conocimientos adecuados y mal intencionados puedan descubrir estos agujeros y ejecutar ataques cada vez mas complejos.

Por otra parte no se tienen actualmente aplicaciones de seguridad como *firewalls* para proveer protección a nivel L3 con IPv6. Aunque existe una gran cantidad de empresas de software que producen estos programas, están dirigidos al bien conocido direccionamiento IPv4. Debido a la escasez actual de redes comerciales IPv6 no existe aún el estimulo económico para el desarrollo de estas herramientas de protección.

El uso de la dirección MAC en el campo host ID de una dirección IPv6 representa una amenaza a la privacidad, ya que éste es un identificador de interfaz único a nivel mundial, resulta fácil relacionarlo con un usuario en particular, lo que permitiría o bien facilitaría la elaboración de perfiles no autorizados contentivos del tipo de actividades de este en la red, como lo son páginas HTTP visitadas, comunicaciones telefónicas, envío de correos, horarios de conexión entre otros. Hasta los momentos estas actividades se observan en aplicaciones de L7 mediante la instalación no autorizada de *cookies* y programas espías en los hosts, que sin embargo son relativamente fáciles de mantener bajo control.

Los ISP que mantengan hosts únicamente IPv4 una vez se agoten las reservas de estas direcciones, deberán implementar mecanismos de traducción como NAT-PT *(NAT-Protocol Translation),* debido a que ya no existirán nuevos hosts con ambos protocolos coexistiendo *(dual stak)* sino que serán IPv6 solamente, por lo que al no poseer una dirección IPv4 se imposibilita la conexión entre ambos, como podrían ser el caso de un servidor HTTP y un computador personal que intenta acceder a el.

4.2 Estrategias de Transición Aplicables

En el proceso de migración no necesariamente se deben actualizar todos los nodos de red al mismo tiempo. Las características de la corporación o ISP que se encamine en dicho proceso dictaminará las estrategias y técnicas a usar para lograr una transición lo más transparentemente posible al usuario o cliente y en coexistencia con IPv4.

Existen diversas técnicas para la implementación de IPv6, las cuales pueden usarse en combinación según las circunstancias de la red. A continuación se describen las mas usadas actualmente.

4.2.1 Dual Stack

Doble pila en L3, los nodos configurados de esta manera pueden manejar ambos protocolos, esto significa que sus interfaces poseen tanto una dirección IPv4 como direcciones IPv6, por lo que pueden tener conectividad con cualquier red IP. Los nodos deciden que pila usar en base a la versión de la dirección de destino en el paquete que reciben, en el caso de host también en la respuesta DNS (la cual no necesariamente debe concordar con el protocolo que se usó para transportarla) y de las preferencias de la aplicación implicada.

Lo ideal o lo que se debe intentar es que todo nodo soporte la doble pila de L3; sin embargo, esto no es siempre posible, por costos o limitaciones de hardware entre otras causas. De esta manera se tiene funcionalidad total de QoS, seguridad, multicast, gestión y rendimiento.

Esta estrategia será el norte a seguir en proceso de migración en CANTV, puesto que no se requerirán cambios de hardware. La limitante serán las actualizaciones de software bajo licencia que se requerirán y se tratarán de minimizar.

4.2.2 Túnel 6to4

Mediante esta técnica se pueden interconectar islas IPv6 a través de redes IPv4, para esto se requiere que los routers de borde de la red IPv6 sean dual stack de manera que los paquetes v6 son encapsulados con cabeceras v4 permitiendo que sean reenviadas a través de la red hasta su destino final, donde existe otro router de borde dual stack que desencapsula el paquete IPv6 y lo reenvía hacia la red v6. A su vez alguno de estos routers puede funcionar como un agente de relevo para conectarse a una internet puramente IPv6.

Para su funcionamiento los hosts o routers dual stack de borde (que están atados a redes en base a un pool de direcciones IPv6 especiales con prefijo 2002:/16) y cuya interfaz de estos con la red IPv4 esta configurada con una dirección global que a su vez es mapeada al prefijo v6 /48 como se muestra en la *figura 4.1*. (para este ejemplo se usaron direcciones privadas IPv4)

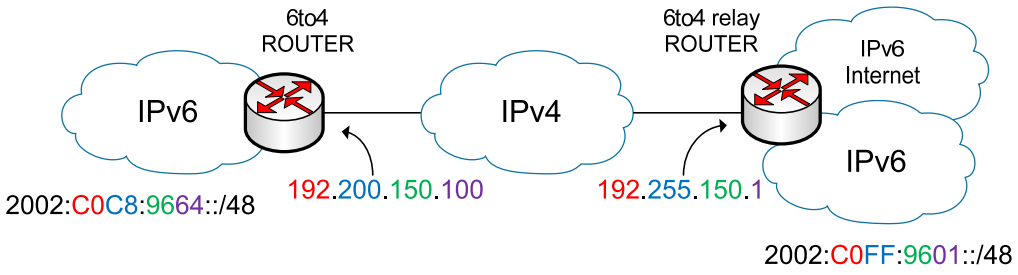


Figura 4.1 Túnel 6to4. Fuente: Autor

Estos túneles se establecen dinámicamente por lo que no requieren configuración previa. En CANTV sería sencillo implementar este tipo de túneles configurando los routers BRAS únicamente, luego cada cliente ABA con sistemas operativos como Windows XP o superior obtendrían sus direcciones de prefijo 2002::/16 automáticamente a partir de la dirección IPv4 asignada normalmente, logrando una conexión parcial a internet v6, ya que ésta será solo a las islas que

dispongan de routers y hosts 6to4. IPv6 multicast no opera en estos túneles y como se puede observar esta estrategia depende totalmente del direccionamiento IPv4 por lo que se evitará sus uso en la corporación.

4.2.3 ISATAP

Intra Site Automatic Tunnel Addressing Protocol, permite conectar nodos dual stack en una red IPv4 generando una dirección IPv6 con un prefijo ISATAP /64 a partir de una dirección IPv4. Esta última es mapeada en los bits menos significativos del campo *interface ID* de la dirección IPv6, mientras que los 32 bits más significativos restantes de este campo están conformados por :0000: 5EFE:. El host obtiene el prefijo requerido preguntándoselo a un router ISATAP. Esta técnica usa a IPv4 como si se tratara de un protocolo L2 que le brinda conectividad con la red IPv6 como se muestra en la *figura 4.2*:

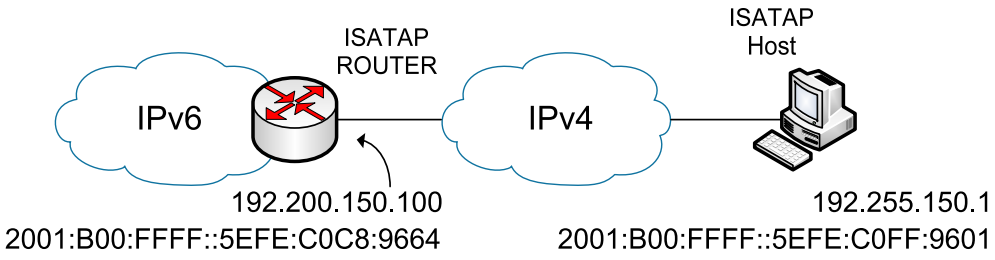


Figura 4.2 ISATAP

El router ISATAP encapsula los paquetes IPv6 en IPv4, de manera que la red IPv6 observa a la IPv4 como una red v6 de prefijo 2001:B00:FFFF::/64 y los hosts observan al router ISATAP como si estuvieran conectados directamente a el.

Es una manera sencilla para los clientes ABA de obtener conectividad a redes IPv6 que solo requiere de la configuración de sus propios hosts o sus propios routers, Sin embargo tiene las mismas desventajas de 6to4 cuando solo ofrece conectividad entre nodos ISATAP a través de redes IPv4. Es una técnica que está más dirigida a

los clientes de CANTV más que a la propia corporación, por lo que su uso queda descartado para la migración. Por otra parte, los host deben poseer sistemas operativos capaces de soportar esta función, la mayor parte de las distribuciones Linux y OpenBSD no lo hacen.

4.2.4 NAT-PT

NAT Protocol Translation permite que el router en donde se esté ejecutando intercambie la cabecera IPv4 de un paquete entrante por una interfaz únicamente v4 por una cabecera IPv6 para luego ser reenviado a una red IPv6 nativa y viceversa. Esto permite que hosts únicamente v4 tengan conectividad con host únicamente v6 pero con un alto precio de seguridad, gestión compleja, pobre aplicación de QoS, además de todos los problemas de NAT. Debe ser usado como último recurso en el caso de que en el proceso de migración queden hosts IPv4 que no se puedan actualizar a dual stack.

En la corporación no existen nodos de red que no puedan ser dual-stack o por lo menos no se requiere que accedan a IPv6, por lo que esta técnica también puede ser descartada.

4.3 Proceso de Migración en CANTV

Para que la corporación ingrese al mundo IPv6 debe seguir una serie de pasos o *roadmap*, que como se describirá mas adelante algunos deberán ejecutarse lo mas rapidamente posible, mientras que con otros se puede esperar al momento mas adecuado.

4.3.1 Obtención y Plan de Asignación de un Bloque IPv6

Se trata del primer paso forzoso. Estas deben ser solicitadas a LACNIC la cual a diferencia de IPv4 las otorga sin el cobro de ningún tipo de tasa, en aras de estimular el proceso de implementación. Esta otorga bloques de direcciones globales con prefijo /32 los cuales estos últimos dejan 16 bits para que CANTV cree sub-redes propias, lo cual implica una capacidad máxima teórica de 65.536 de estas. A partir de esto se delegan subredes a los clientes corporativos (que pueden o no usar el campo subnet ID completo) y a los servicios, para estos últimos se cuenta además con todo el campo subnet-ID por lo que se tendrían otros 16 bits de direccionamiento. Con esto se le puede crear no solo cuatro direcciones exclusivas, sino una sub-red exclusiva para cada habitante de Venezuela, aunque es claro que esta no es la idea si se puede percibir que la asignación /32 es suficiente.

La solicitud de la asignación del bloque /32 se realiza mediante el llenado y envío de un formulario hallado en la página web de LACNIC, en el cual se solicitan los datos de CANTV además de anexar el plan de uso, plan de asignación de direcciones y la estructura de la red IPv6.

El plan de asignaciones deberá ser diseñado a partir de los servicios, la distribución geográfica y la densidad de clientes por área, además en la medida de lo posible deberá cumplir con los siguientes objetivos:

- Prevenir que a la hora de ampliar las asignaciones, estas sean contiguas a las asignadas inicialmente.
- Estas deben ser lo suficientemente grandes como para evitar nuevas asignaciones de manera frecuente.
- Aunque se cuenta con una cantidad enorme de direcciones, se debe evitar el desperdicio de las mismas.
- Se debe determinar fácilmente con una simple inspección visual, a que localidad pertenece una dirección.

Para los routers y servidores es recomendable el uso de direcciones site-local (FEC0::/10) que además de permitir su rápido reconocimiento, no son accesibles desde fuera de la organización. Para esto se debe crear un plan de asignaciones con los 54 bits del campo subnet-ID en base al tipo de dispositivo y su ubicación en la red.

4.3.2 Migración del Back-Bone

El hecho de que este funcione bajo MPLS conlleva una enorme ventaja para el momento de la migración. Como se explicó antes, los router LER que se encuentran en el borde del mismo son los que se encargan de etiquetar y desetiquetar los flujos de datos y que por lo tanto toda configuración del back-bone se debe realizar en los mismos. Si se convierte a dual-stack solo los routers LER y se configuran para crear LSP para los datagramas IPv6, el resto de los routers internos pueden quedar sin ningún tipo de cambio, ya que estos enrutarán estos mensajes en base a las etiquetas impuestas por los LER. Esta técnica llamada 6PE *(6 Provider Edge)* permite tener un back-bone para IPv6 con un impacto de migración mínimo en el mismo, ya que entre otras cosas se puede evitar el uso de túneles y mecanismos de traducción.

Lo mas recomendable es mantener el IGRP actual o OSPFv2 para los router internos y OSPFv3 para los dual-stack, ambos pueden coexistir sin problemas. IS-IS es apropiado para redes de mayor tamaño y no ofrece beneficios superiores a los de OSPF, por otro lado requeriría de entrenamiento de personal y cambio en la distribución de las áreas, ítems que no se requerirían con OSPFv3. Por otro lado los routers de borde de internet deberán ser además configurados con BGPv4 como EGP; dicho proceso de debe realizar en conjunto con los distintos proveedores de acceso internacional. En la *figura 4.3* se aprecia un ejemplo del funcionamiento de 6PE.

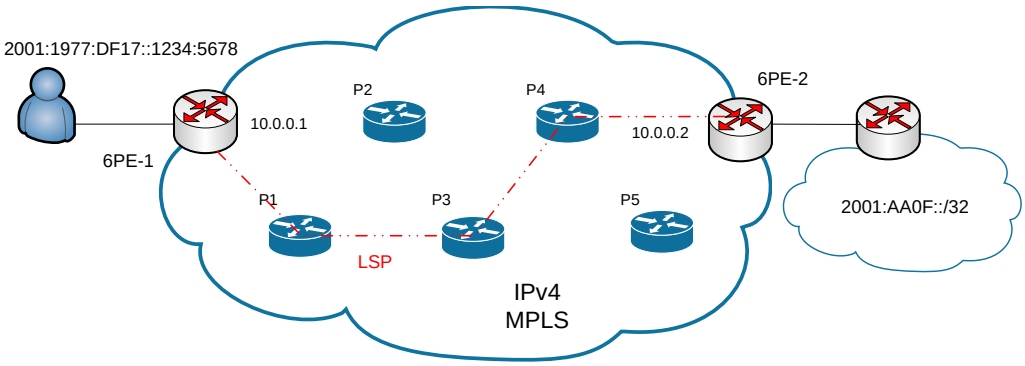


Figura 4.3 6PE. Fuente: Autor.

El usuario IPv6 requiere alcanzar la red 2001:AA0F::/32, para esto los routers 6PE-1 y 6PE-2 conocen del alcance a esta red mediante OSPFv3; luego dentro del back-bone MPLS IPv4 se construye un LSA en base a la información obtenida mediante OSPFv2 que indica el alcance de 10.0.0.1 con 10.0.0.2. Los routers P transmiten los mensajes OSPFv3 sin leerlos.

Con este método sólo se requiere actualizar los sistemas operativos de los routers 6PE; en cambio, la red MPLS para IPv4 no se ve afectada en ningún modo y se ven minimizados los costos de migración. Los routers 6PE se pueden añadir por grupos o por unidades en cualquier momento. Para CANTV lo mas recomendable en una primera etapa de migración es adaptar al back-bone de manera de brindar acceso a internet v4/v6, para esto solo bastaría actualizar los routers en la *figura 4.4*

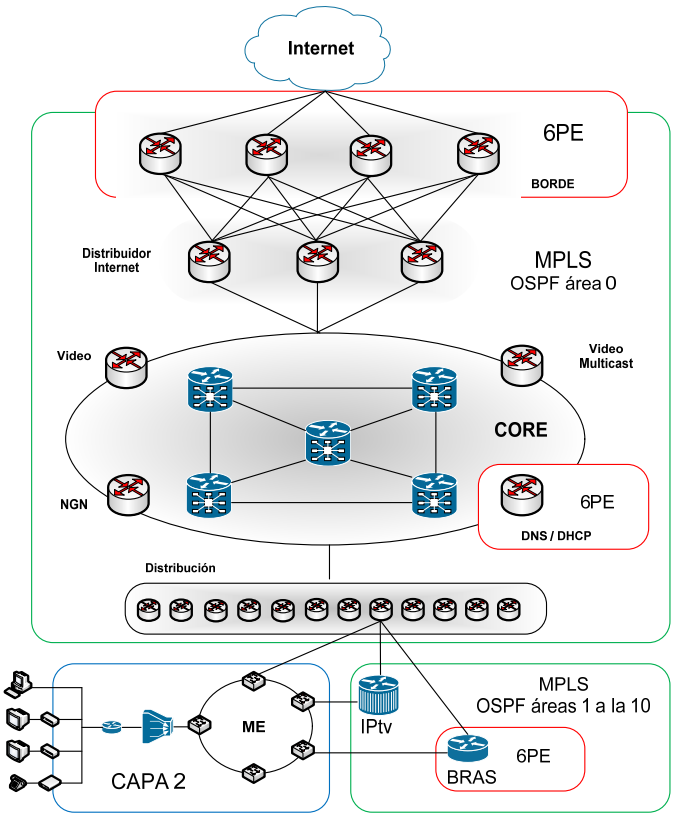


Figura 4.4 Primera Etapa de Migración. Fuente: Autor.

El proceso de actualización del sistema operativo se realiza en cuestión de horas y su configuración puede ser preestablecida para evitar retrasos en la puesta en servicio del mismo. El primer paso para realizar la actividad consiste en desviar el tráfico al sistema redundante, por tal motivo debe ser efectuado en los momentos de menor flujo de tráfico. Una vez realizada la actualización del sistema operativo y culminado todo el protocolo de pruebas, se debe realizar el mismo procedimiento al sistema redundante. Cabe destacar que el protocolo de pruebas debe ser realizado por el personal de Cisco Systems, Juniper y avalado por CANTV, debido a la pluralidad del equipo que se encuentra involucrado.

El protocolo de pruebas debe constar tanto del ya usado actualmente, además del envío de flujos IPv6 a través de la MPLS entre los LER de la misma, midiendo la latencia o tiempo de tráfico de los mismos. Una vez se tengan varios 6PE en el backbone las pruebas se deben enfocar al funcionamiento de OSPFv3 midiendo los tiempos en que la red v6 alcanza la convergencia (los routers actualizan sus tablas de ruteo IPv4/v6).

4.3.3 DNS y DHCP

En primer lugar se deben convertir a 6PE los router de agregación al core de estos servidores así como activar el nuevo protocolo en sus sistemas operativos antes descritos, para entonces asignarles direcciones IPv6 fijas.

Para disponer de DHCPv6 se debe hacer la actualización de Cisco CNR 6.2.3 a 7.0.1 en los 4 servidores DHCP y sus respectivos servidores redundantes. Este programa no varía mucho de la versión anterior, esto es, la manera de configurar políticas y opciones mediante las cuales se asignan los pool de direcciones IPv6 de acuerdo al plan de asignaciones previamente establecido.

Es recomendable abandonar el uso de la dirección MAC para el campo interface ID como medida de seguridad y en su lugar establecer una numeración para cada prefijo /64 asignado; este debe cambiar cada vez que se renueve la dirección de cada host.

Los servidores DNS ya ejecutan BIND 9.4.2 por lo que están listos para resolver direcciones URL para IPv6; de hecho, actualmente si se realizan consultas (por ejemplo mediante el nslookup, set q=any) se obtienen respuestas para v6. Queda entonces añadir los registros AAAA propios o autoritativos de la corporación, estos se añaden al servidor SOA bajo las siguientes premisas:

- La dirección de IPv6 ha sido asignada a por lo menos una interfaz del nodo donde se ofrece el servicio.
- La dirección está configurada en la interfaz.
- El nodo tiene conectividad a la infraestructura de IPv6.

Una vez se logre tanto la adecuación del back-bone como la configuración de los servidores DHCP y DNS, los clientes ABA con sistemas operativos dual-stack, pueden entonces acceder a servicios IPv6 vía internet como lo son páginas web únicamente v6.

4.3.4 Voz sobre IP y NGN

Este servicio resulta sencillo de migrar. Tanto el software como el hardware que lo componen operan con SIPv2, por lo que bastaría solo con configurar los

servidores DHCP con los respectivos pools de direcciones para este servicio de la misma manera descrita en el punto anterior, la base de datos *Oracle* del OCMP que debe ser reprogramada ahora con campos contentivos de las direcciones IPv6 y el router de agregación al core para NGN debe ser convertido a dual stack 6PE.

Por los momentos no hay una necesidad urgente de realizar esta migración, sin embargo se debe hacer para garantizar el funcionamiento del servicio en unos estimados 4 años cuando ya no existan direcciones IPv4 y los nuevos clientes VoIP a nivel mundial sean puramente IPv6, dado que este no funciona bajo mecanismos de traducción como NAT-PT.

Las redes NGN para el tráfico de voz PSTN a través de la red metro ethernet y backbone se recomienda mantenerlas IPv4, dado que la tendencia mundial para este tipo de servicio apunta a VoIP bajo SIP. La corporación deberá migrar a este protocolo a los clientes de voz aunque no contraten ABA. Sin embargo, este proceso puede realizarse implementando IPv6 de manera nativa cuando las inversiones en tecnologías PSTN como las centrales SS7 y Huawei UA hayan cumplido su vida útil.

4.3.5 Televisión vía IP

Este servicio aún en desarrollo usará direcciones privadas unicast para el servicio VoD y direccionamiento multicast para los canales provenientes de los encoders en el headend de Camatagua. Esto lo convierte en un servicio estrictamente interno a la red de la corporación, de esta manera ha sido concebido y las capacidades de direccionamiento de IPv4 tanto unicast como multicast cubren las expectativas de capacidad requeridas. Cabe recordar también que el direccionamiento privado y multicast (de alcance local) no representan un gasto de direcciones IPv4.

La aplicación de IPv6 en ambos ámbitos puede mantenerse en espera hasta que el crecimiento de la red IPtv crezca de manera tal que se requiera ampliar las capacidades de direccionamiento, mediante prefijo site-local (FEC0::/16) o mediante direcciones global unicast si para el momento las políticas del servicio cambian y se permitirá el acceso a trafico externo a la red, así también para las direcciones IPv6 de multicast.

La aplicación de IPv6 puede coexistir con IPv4 y esta requerirá de configurar como dual-stack los STB y el CPE; este último aunque trabaja en modo *bridge* para todos los servicios, trabaja en modo router para la gestión por lo que su interfaz con la línea de abonado debe poseer una dirección IP. Los switches Alcatel-Lucent 7450 ESS deben ser configurados también como dual-stack y configurados con MLD

v1/v2 para que puedan propagar el tráfico multicast. Como con todos los demás servicios todos los routers deben ser configurados como 6PE.

4.3.6 Interconexión WAN

Como se trató anteriormente, se recomienda la creación de una VPLS estática por cliente que interconecte los diversos CPE de cada locación de los mismos, de esta manera se transportarán las tramas ethernet contentivas de IPv6, IPv4 (o cualquier otro protocolo como Apple talk o IPx). Al ser la VPLS estática los router PE de la corporación no requerirán mas que leer la dirección MAC de destino en el paquete proveniente de la red metro ethernet y compararla con una tabla fija para localizar el PE de destino y realizar el envío de la trama ethernet a través de MPLS.

4.4 Siguientes Pasos

El backbone mediante 6PE se comporta como dual stack; sin embargo internamente no responde correctamente a comandos ICMPv6 como *ping6* y *tracert*, usados por el personal de gestión para la resolución de problemas y monitoreo de la red. Sin embargo este problema puede ser resuelto mediante mediciones in situ y técnicas de L2 por lo que lo recomendable es que la migración total del backbone se realice al mismo momento que se requiera su actualización por motivos de saturación de tráfico o sea el fin de la vida útil de los elementos de software o hardware que lo componen. Actualmente todo nodo de red que aparece en el mercado esta preparado para IPv6, es *IPv6 ready*.

CONCLUSIONES

El agotamiento de las capacidades de direccionamiento IPv4 con unas $4*10^9$ direcciones es el mejor indicativo del vasto crecimiento de las redes IP en la red global, el cual cada año apunta crecer de manera mas acelerada, de forma que la experiencia de vida humana se vera afectada por una gran cantidad de dispositivos conectados a la red. Estos van desde teléfonos móviles, hasta sensores en diversas partes del hogar, la oficina e inclusive dentro del organismo humano como dispositivos médicos.

IPv6 fue desarrollado desde el momento en que el agotamiento de IPv4 se vio venir; su principal premisa fue solucionar este problema y evitar que se repita en varias generaciones. Siendo un protocolo diseñado veinte años después que su predecesor y con la experiencia comercial del mismo, trae consigo una serie de mejoras las cuales, en su mayoría, se aplican a IPv4 mediante aplicaciones y protocolos "anexos" a este. Por todo esto IPv6 mas que una mejora a la red global debe ser visto como una solución a un problema de capacidad de expansión de la misma.

El nuevo protocolo nace atendiendo al problema de la migración el cual implica la coexistencia con IPv4. La consigna a seguir por los operadores de red sería *"dual stack donde se pueda, túneles en todo lo demás"*. Las diversas experiencias en redes académicas y de investigación como la 6bone, abren ahora la puerta al uso comercial de este protocolo que resulta un paso forzado para cualquier organización, ISP y proveedores de redes de transporte, que requiera mantener sus servicios acorde con las exigencias mundiales.

CANTV se encuentra en una posición privilegiada para realizar la migración. Dado que el cambio del viejo esquema PSTN a NGN se realizó relativamente hace poco tiempo, las tecnologías usadas son fácilmente actualizables sin la necesidad de requerir cambios de hardware, los cuales son mas costosos e impactan de manera mas

profunda a la prestación de los servicios. Está también el hecho de que la red de distribución y última milla, en este caso la metro ethernet y DSL, las cuales conforman la mayor parte de toda la red de la corporación son dispositivos de L2 para los cuales IP les es tranparente, exceptuando para el servicio IPtv de muticast el cual aun no ha sido desplegado.

El backbone MPLS, resulta ser una enorme ventaja al poder convertirlo a dual stack migrando solo unos cuantos componentes del mismo mediante la técnica 6PE, lo que representa un ahorro sustancial de costos y facilita el proceso de migración. Otro beneficio es que se omite la necesidad de aplicar túneles, los cuales están llenos de limitaciones y requieren de una gestión especial.

Ambos bordes de la red, hosts y compañías de transporte afortunadamente están listas desde hace ya unos pocos años para el nuevo protocolo. Una vez que se obtenga el prefijo IPv6 por parte de LACNIC, se configuren los servidores DHCP y DNS además de migrar el backbone, se podrá tener acceso a la internet v6, que aunque hoy en día es mínima y carente de servicios como la v4, de manera inevitable y dentro de no muchos años la situación se revertirá.

RECOMENDACIONES

Una vez analizada la red de datos CANTV mediante este estudio se puede observar la factibilidad de la migración a IPv6 mediante los métodos nombrados en el mismo por lo que se plantean las siguientes recomendaciones.

1. Entrenamiento apropiado y oportuno del personal de ingeniería en la corporación en el protocolo IPv6, con énfasis en el área trabajo que corresponda.

2. Al momento de comenzar el diseño de un nuevo servicio o ampliación de la red, esta debe hacerse pensando en IPv6 como un protocolo nativo del mismo.

3. Una vez exista conectividad IPv6 para los clientes CANTV, se debe crear una página HTTP puramente v6, con el objetivo de que los mismos puedan verificar su propia conectividad mediante IPv6. Para esto la página puede contar con aplicaciones para tal fin.

REFERENCIAS BIBLIOGRÁFICAS

[1] Forouzan, Behrouz A. *Transmisión de Datos y Redes de Comunicaciones*. Mac Graw Hill, segunda edición (2002).

[2] Wikipedia. *TCP/IP* - **EN:** http://en.wikipedia.org/wiki/Tcp/ip/.- Enciclopedia en Línea, (2007). [Consulta: 2008, Noviembre].

[3] Root Servers Technical Operations Assn. *Root Servers* –**EN:** http://www.root-servers.org/ - [Consulta: 2008, Octubre].

[4] Cisco. *Cisco Certified Network Associated*. – **EN:** CCNA semestre 1, versión 4.0, 2008.

[5] Davies, Joseph. *Understanding IPv6.* Microsoft Press, segunda edición.(2008).

[6] CANTV. *La Empresa* -**EN:** - http://www.cantv.com.ve/seccion.asp?pid=1&sid=1861&id=2&und=6&cat=item_lc&item=item_2&item_name=Misi%F3n [Consulta: 2008, Noviembre].

[7] CANTV. *Jornada Tecnológica y de Implantación.* – presentación – Caracas: Gerencia de Ingeniería y Construcción de Redes, 2005.

[8] Wikipedia *ADSL* –**EN:** http://en.wikipedia.org/wiki/Adsl Enciclopedia en Línea, (2007). [Consulta: 2009, Marzo].

[9] Global Crossing. *Interactive Map* –**EN:** http://www.globalcrossing.com/network/network_interactive_map.aspx. - [Consulta: 2008, Diciembre].

[10] LACNIC. *Consumo de IPv4 y la Transición a IPv6* – presentación – Washington DC, USA: Campaña América Latina y Caribe en IPv6, Marzo 2008.

[11] State Key Laboratory. *AS Level IPv6 Backbone Network Topology* –**EN:** http://ipv6.nlsde.buaa.edu.cn/ - [Consulta: 2008, Diciembre].

[12] ARBOR Networks. *Worldwide Infrastructure Security Report* - **EN:** http://www.arbornetworks.com/report - Página Web de ARBOR Networks (2008) [Consulta: 2009, Enero].

BIBLIOGRAFÍAS

Forouzan, Behrouz A. *Transmisión de Datos y Redes de Comunicaciones*. Mac Graw Hill, segunda edición. España, 2002.

Davies, Joseph. *Understanding IPv6.* Microsoft Press, segunda edición. USA, 2008.

Silvia, Hagen. *IPv6 Essentials.* O´Reilly, segunda edición. USA, 2006.

Stockebrand, Benedikt. *IPv6 in practice.* Springer, primera edición. Berlín, 2007.

Sam, Halabi. *Metro Ethernet.* Cisco Press, primera edición. USA, 2003.

Cisco. *Cisco Certified Network Associated*. CCNA semestre 1, versión 4.0, 2008.

CANTV. *Jornada Tecnológica y de Implantación.* – presentación – Caracas: Gerencia de Ingeniería y Construcción de Redes, 2005.

Entrevistas realizadas al personal de Ingeniería en CANTV, Noviembre 2008.

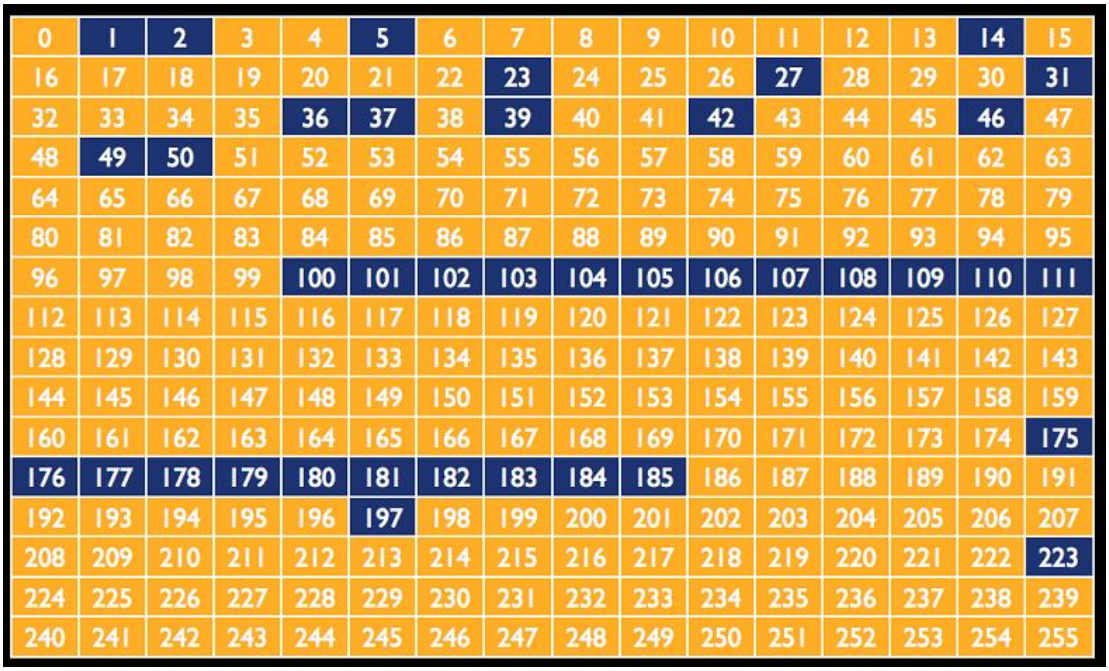
LACNIC. *Consumo de IPv4 y la Transición a IPv6* – presentación – Washington DC, USA: Campaña América Latina y Caribe en IPv6, Marzo 2008

IPv6 Task Force [en línea]. www.ipv6tf.org [Consulta: Noviembre 2008]

Cisco Systems [en línea]. http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html [Consulta: Diciembre 2008]

[ANEXO 1]

[Mapa de ocupación del espacio IPv4]



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

En la figura se observan en color azul los bloques IPv4 /8 que aun no han sido completamente asignados para Octubre del 2008.
[http://www.personal.psu.edu/dvm105/blogs/ipv6/].

[ANEXO 2]

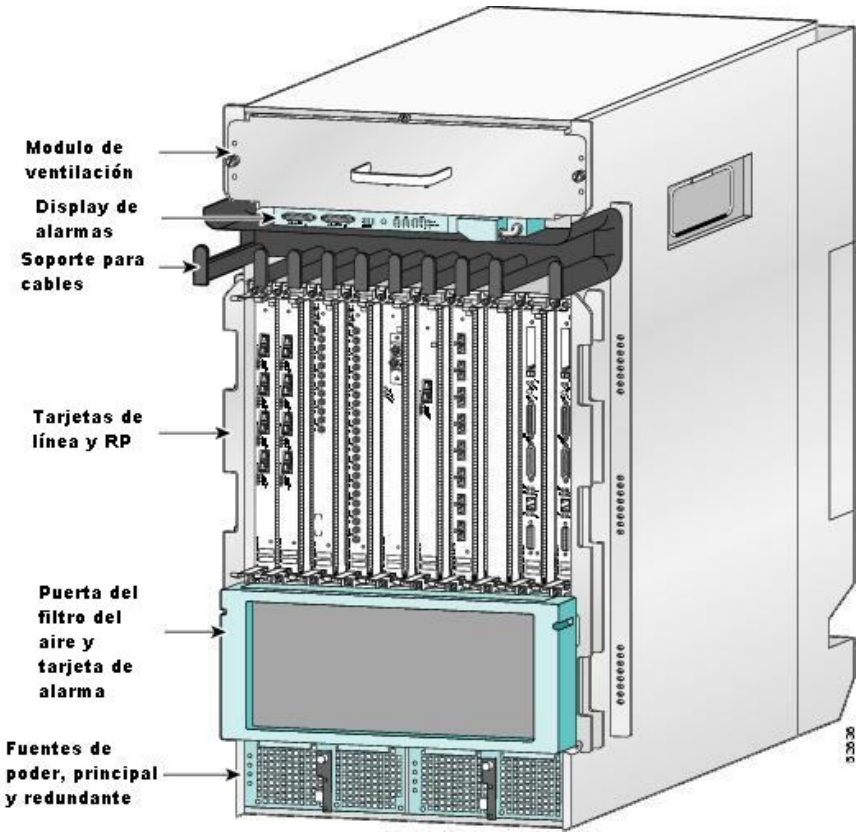
[Cabeceras de Extensión IPv6]

Orden	Tipo de Cabecera	Código
1	Cabecera básica ipv6	
2	Opciones de Salto	0
3	Opciones de Destino	60
4	Enrutamiento	43
5	Autenticación	51
6	Seguridad (encriptación del payload)	50
7	Opciones de Destino	60
8	Movilidad	135
	No hay siguiente cabecera	59
Capa superior	TCP	6
Capa superior	UDP	17
Capa superior	ICMPv6	58

[ANEXO 3]

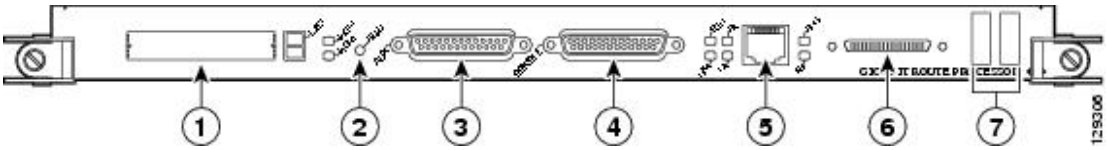
[Routers Cisco y Juniper]

Distribución de los Racks (semejante en ambas marcas)



Las tarjetas de línea representan las interfaces del dispositivo, las cuales pueden ser Ethernet o PPP en fibra óptica (principalmente), UTP *(Unshieled Twisted Pair)* o serial, mientras que las RP *(Router Procesor)* son el router mismo, contienen el procesador y las distintas memorias, así como las interfaces de configuración local. [https://www.cisco.com/en/US/docs/routers/12000/12010s/installation/guide/hfdm_c01.html#wp1126594]

Tarjeta RP (semejante en ambas marcas)



Esta contiene al procesador y las distintas memorias, la memoria flash que contiene al sistema operativo se trata de un modulo intercambiable (1) lo que facilita el proceso de actualización del mismo. En (2) se encuentran los leds indicadores de actividad y el botón de reset, (3 y 4) son los puertos de consola principal y auxiliar, (5 y 6) son puertos ethernet para configuración local (RJ45 y MII respectivamente), finalmente se tienen unos diplays (7) que presentan mensajes de configuración y estado.

[https://www.cisco.com/en/US/docs/routers/12000/12010s/installation/guide/hfdm_c01.html#wp1126594]